Challenges and opportunities in onboarding smart-home devices

Chixiang Wang
Dartmouth College
Hanover, NH, USA

Liam Cassidy
Dartmouth College
Hanover, NH, USA

Weijia He
Dartmouth College
Hanover, NH, USA

Timothy J. Pierson
Dartmouth College
Hanover, NH, USA

David Kotz
Dartmouth College
Hanover, NH, USA

ABSTRACT

Smart-home devices have become integral to daily routines, but their onboarding procedures – setting up a newly acquired smart device into operational mode – remain understudied. The heterogeneity of smart-home devices and their onboarding procedure can easily overwhelm users when they scale up their smart-home system. While Matter, the new IoT standard, aims to unify the smart-home ecosystem, it is still evolving, resulting in mixed compliance among devices. In this paper, we study the complexity of device onboarding from users' perspectives. We thus performed cognitive walkthroughs on 12 commercially available smart-home devices, documenting the commonality and distinctions of the onboarding process across these devices. We found that onboarding smart home devices can often be tedious and confusing. Users must devote significant time to creating an account, searching for the target device, and providing Wi-Fi credentials for each device they install. Matter-compatible devices are supposedly easier to manage, as they can be registered through one single hub independent of the vendor. Unfortunately, we found such a statement is not always true. Some devices still need their own companion apps and accounts to fully function. Based on our observations, we give recommendations about how to support a more user-friendly onboarding process.

KEYWORDS

smart-home, device onboarding, user experience, Matter

ACM Reference Format:
Chixiang Wang, Liam Cassidy, Weijia He, Timothy J. Pierson, and David Kotz. 2024. Challenges and opportunities in onboarding smart-home devices. In *The 25th International Workshop on Mobile Computing Systems and Applications (HOTMOBILE '24), February 28–29, 2024, San Diego, CA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3638550.3641137

1 INTRODUCTION

Smart-home devices are increasingly becoming integral components of individuals' daily routines, with major corporations manufacturing a wide array of devices from televisions to thermostats, from lightbulbs to speakers, from door locks to smoke alarms. In contrast to mobile phones, the process of onboarding a smart-home device lacks a clear and well-researched approach due to variations in device capabilities and operating procedures. We define the ***onboarding*** of a smart-home device as the process of setting up a newly acquired smart-home device – from the moment it comes out of the box until it is fully operational. This process includes hardware installation or assembly, pairing with the user's control device (typically a smartphone), establishment of connections with the user's home network or other middlebox (typically a hub), and device configuration. In short, onboarding a smart-home device makes it part of the home's infrastructure.

Making things even more complex, many devices require their own branded app to set up and control. This situation means that when consumers intend to onboard a number of different smart-home devices in their home, unless they limit their purchases to a single brand (which often cannot satisfy consumer needs), they must install numerous different smart-home apps in their phones! Even smart-home devices under the same brand may rely on different communication methods and procedures. For example, some devices may connect to the cloud via Wi-Fi, others may connect to a hub using Bluetooth, some devices may communicate directly with each other using Thread, and so on. In practice, each of these communication strategies leads to different requirements and processes when onboarding devices.

Furthermore, researchers anticipate a huge increase in the prevalence of smart devices in households. While the task of onboarding a few smart devices may require only ten or twenty minutes, the prospect of dealing with dozens or even hundreds of devices imposes a significant burden of time and effort. Consumers need a streamlined and user-friendly approach to device onboarding.

A new initiative called Matter [2] (previously called CHIP) launched in 2023 and aims to create a unified onboarding process. While Matter is a step in the right direction, the protocol is still evolving and is not yet widely deployed. In fact, we observed certain newly produced devices that claim to be Matter-compatible; however, they necessitated an old-school onboarding process through their own branded app before undergoing a firmware update, subsequently enabling Matter capabilities – which makes consumers more confused (see Section 4). Furthermore, many current commercially available smart-home devices still lack support for Matter. Understanding the current state of commercially available smart-home home devices is important for deploying practical systems. We address that shortcoming in this paper.

Previous research on user experiences with smart homes has predominantly concentrated on usability [12, 18], security [15, 19], privacy [1, 15], and device lifecycles [8, 16, 20]. Remarkably, the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
HOTMOBILE '24, February 28–29, 2024, San Diego, CA, USA
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0497-0/24/02…$15.00
https://doi.org/10.1145/3638550.3641137

user experience associated with onboarding smart-home devices has remained relatively underexplored.

In this paper, we investigate the onboarding process of 12 commercially available smart-home devices. More specifically, our investigation aims to answer the following research questions.

- **RQ1:** What are the onboarding processes for contemporary commercially available smart-home devices?
- **RQ2:** What challenges do consumers typically encounter during the onboarding process?
- **RQ3:** What strategies can be employed to enhance the user experience for onboarding smart-home devices?

To answer these research questions, we performed cognitive walkthroughs on the onboarding process of each device, documenting everything we did and observed during the walkthroughs. By analyzing the documented logs, we acquire insights into the common designs shared by vendors as well as the distinct methods they used. For example, today's smart home devices are managed via a smartphone app. To communicate with the app, the device must be paired with the app and, in some cases, with the smartphone. The pairing methods, however, can differ from vendor to vendor.

By identifying commonalities and distinctions across apps and approaches, we exposed pros and cons concerning user experience; this paper outlines usability hurdles and offers potential solutions. For instance, the device pairing process could either be initiated by the user or the device itself. When comparing the two approaches, we found that the device-initiated pairing method greatly minimizes the strain placed on the user, as it frequently omits the necessity of locating the proper device model in a long list on the app. From this and other observations, we curate a list of suggestions for future smart-home researchers and system designers.

2 RELATED WORK

In this section, we summarize related work and examine onboarding from a system and user perspective.

2.1 System perspective

While there are differences in approach between different vendors, from a system's point of view, the purpose of onboarding a smart home device is often to establish a secure connection between three parties: a new device, the companion app on a smartphone, and the manufacturer's cloud [3, 20]. Given that the device was previously unknown to the companion app and the cloud, recognizing the correct device becomes a significant challenge. The onboarding process often involves five distinct stages: device discovery, Wi-Fi provisioning, device pairing, device registration, and authorization [20]. Unfortunately, the complicated process makes the smart home implementation error-prone. Furthermore, prior papers have identified vulnerabilities in the onboarding process that expose attacks such as device impersonation [14]. Clearly, securely introducing new devices should be an important goal of device onboarding.

Security is not the only concern, however. The complicated onboarding process also leads to various implementations by different smart home vendors, causing an interoperability problem. Any smart home platforms that try to unify the fragmented market have to make extra effort to be compatible with existing implementations. For example, Google Home provides three different protocols for device discovery, including mDNS, UPnP, and UDP, to appeal to existing smart-home products, making it possible to onboard various smart-home devices [11]. Similarly, many smart devices attempt to be compatible with multiple smart-home platforms (e.g., Google Home, Apple HomeKit, Samsung SmartThings), and each platform has its own set of protocols. It is not easy to implement all these protocols correctly; bugs lead to user frustration or insecure operation.

2.2 User perspective

Surprisingly, little research has been done on the obstacles users face in smart-home device onboarding. Most prior work focuses on difficulties that occur while smart devices are in use [7, 8, 15, 18], which are often different from the challenges of introducing a new device to the home system.

For the few works that focus on the onboarding process, one can conclude that device onboarding not only causes trouble for smart-home vendors, but also frustrates smart-home users. Jakobi et al. conducted an 18-month Living Lab study that shows that users often have trouble with connecting devices to the gateway [12]. Oliveira et al. also found that technical difficulties in hardware and software are a major block for lay users to realize smart homes [4]. Indeed, any trivial hiccup can soon become annoying when the smart-home system scales [8]. These studies were conducted more than five or ten years ago, and the technology has evolved quite a bit since then. It is time to refresh our knowledge on such a topic, especially since the first batch of matter-compatible devices was just made commercially available.

3 METHODS

In this section, we describe our methods, which include how we chose the smart-home devices for this study, as well as how we collected and analyzed user-experience data.

3.1 Device selection

We selected 12 commercially available smart-home devices shown in Table 1. In our selection, we cover a wide range of common categories on the market (hub, camera, switch, bulb, plug, power strip, weather sensor, contact sensor), Matter-compatible and non-Matter-compatible devices (5 non-Matter devices and 7 Matter devices), Wi-Fi devices and non-Wi-Fi devices, Thread devices and non-Thread devices, devices from different manufacturers, and devices that support different platforms (e.g., Apple Home [9], Google Home [10]).

3.2 Data collection

For consistency, one researcher with little experience onboarding smart-home devices collected our entire data set. The researcher was given the 12 selected commercially available smart-home devices as stated above and a private Wi-Fi network to do the study. The researcher kept meticulous notes on the entire onboarding process, including recording every action, prompt, and all other details that happened during the process.

Table 1: The basic information of the devices we used in this study.

No.	Model	Matter-compatible	Supported Platform				Wireless Protocol		
			Google Home	Apple Home	Alexa	SmartThings	Wi-Fi	Bluetooth	Thread
D1	Kasa Smart Wi-Fi Power Strip	No	✓		✓	✓	✓		
D2	Kasa Smart Wi-Fi Light Switch	No	✓		✓	✓	✓		
D3	Kasa Spot 24/7 Recording Camera	No	✓		✓		✓		
D4	Amazon Basics Smart Outdoor Plug	No			✓		✓		
D5	Eve weather: Connected Weather Station	No		✓				✓	✓
D6	Eve door & window: Wireless Contact Sensor	Yes	✓	✓	✓	✓			✓
D7	Amazon Echo Dot	Yes			✓		✓	✓	
D8	Google Nest Hub (2nd gen)	Yes	✓				✓	✓	✓
D9	Nanoleaf Essentials Matter Smart Bulb	Yes	✓	✓				✓	✓
D10	Aqara Hub M2	Yes		✓			✓	✓	
D11	Aqara Door and Window Sensor P2	Yes	✓	✓	✓	✓		✓	✓
D12	Tapo Smart Wi-Fi Light Switch	Yes	✓		✓	✓	✓	✓	

For each device, the researcher first unboxed it, taking out the device itself and other components or accessories (if any). Next, the researcher read the user manual (if any) whether on paper or online. The researcher then followed the user manual to onboard the devices. Each smart-home device in our study required a smartphone to pair with the device for configuration. The researcher paired with an Android phone or an iPhone, recording a written narrative log for each device/smartphone combination.

In some cases, onboarding failed. The researcher made a good-faith effort to solve the problems by changing mobile phones, changing hubs, changing paired apps, and so forth. Each problem mitigation step was carefully recorded.

4 RESULTS

In this section, we elaborate on the results obtained by analyzing the logs, and answer the three research questions we proposed in Section 1.

4.1 RQ1: Onboarding processes

After completing the onboarding process for each device, we analyzed the researcher's logs. We summarize the onboarding process for all devices in Table 2. We divide the smart-home device onboarding procedure into the following steps: preparation, app configuration, device pairing, and device configuration.

4.1.1 Preparation. The first step of onboarding is to prepare the hardware or software required by a smart-home device.

Most devices in our study talk to smartphones through Wi-Fi or Bluetooth and do not require extra hardware. D6, however, supports only Thread and thus requires a Thread border router to work. So, it must only communicate with a Thread border router. For our study, we used D8 (Google Nest Hub, 2nd gen), which is a common smart-home device, as the Thread border router.

Each smart-home device we tested in this study required a smartphone app for onboarding. We encountered two types of apps: device-specific companion apps (manufacturer's apps like Kasa, Tapo, Eve, etc.) that work with particular devices of a single brand, or platform apps (Google Home, Apple Home, Amazon Alexa, Samsung SmartThings, etc.) that generally control and manage compatible smart-home devices from a wide range of manufacturers.

Our researcher read the device's user manual and followed the instructions to select and install the app. There were several other factors that influenced whether a companion app is required and which app to use.

Whether the smart-home device was a Matter-compatible device. For Matter-compatible devices, we usually could use either platform apps or their device-specific companion apps (if any) for onboarding. For non-Matter-compatible devices, however, we had to use the device-specific companion app.

Whether we used an Android or iOS phone. Some devices only have a device-specific companion app for one of the two, Android or iOS. For example, D5 is not a Matter-compatible device, a companion app is required, and it is on iOS only.

Devices manufactured by platform providers. Some devices, such as the D4 (Amazon Basic Smart Outdoor Plug), D7 (Amazon Echo), and D8 (Google Nest Hub, 2nd gen), are manufactured by the major platforms, which means their companion apps are platform apps. Thus, we only tested them through Amazon Alexa (or Google Home), respectively.

Device capability. D9 is a Matter-compatible device and can be onboarded with a platform app. Nonetheless, its functionality is restricted without the companion app, resulting in the unavailability of certain advanced features. Therefore, users have to consider using companion apps to harness the complete spectrum of capabilities offered by such devices.

Special cases. In our study, D10 was a special case; it claimed to be a Matter device but, in practice, could not be onboarded through Matter's protocol with a platform app. It could only activate its Matter-related features after onboarding with its companion app and then doing a firmware update through the companion app. We likely purchased an instance of this device produced at an earlier time with an older version of the firmware. These exceptional cases contributed to consumer perplexity during the onboarding process.

4.1.2 App configuration. App configuration after installation is non-negligible, since this step usually contains several necessary processes. We summarize these steps as follows:

Account registration. For platform apps pre-installed on smartphones, there is generally no need to register a new account. These apps automatically use the device's user account. For instance, the

Table 2: Summary of device onboarding results.

No.	Preparation		App Configuration		Device Pairing			Device Configuration		
	Extra Hardware	Companion App	Account Registration	App Permissions Requested	Initiated by Whom	Check Pairing Mode Indicator	Onboarding Payload Retrieval	Connect to Home Wi-Fi	Input Device Info	Firmware Update Prompted
D1	Not required	Required	Required	Location	User	Required	Device Wi-Fi	Required	Name, location	Yes
D2	Not required	Required	Required	Location	User	Required	Device Wi-Fi	Required	Name, location	Yes
D3	Not required	Required	Required	Microphone	User	Required	Device Wi-Fi	Required	Name, location	Yes
D4	Not required	Required	Required	Bluetooth, contacts, camera, microphone	User	Not required	Bar code	Required	Name, location	No
D5	Not required	Required	Not needed	Apple Home, location	Device	Not required	QR code	Not supported	Name, location	No
D6	Required	Optional	Not needed	Apple Home	User	Not required	QR code	Required	Name, location	No
D7	Not required	Required	Required	Contacts, nearby Devices	User	Required	Device Wi-Fi	Required	Location	No
D8	Not required	Required	Required	Camera	User	Not required	QR code	Not supported	Name, location	No
D9	Not required	Optional	Optional	Camera, cloud sync	User	Not required	QR code	Required	Location	No
D10	Not required	Required	Required	Location, Bluetooth, storage, connect with other devices	User	Required	Bluetooth	Required	Name, location	Yes
D11	Not required	Optional	Optional	Camera	Device	Not required	QR code	Not supported	Name, location	No
D12	Not required	Optional	Optional	Camera	Device	Not required	QR code	Required	Name, location	No

Google Home app was typically seamlessly linked to the Google account associated with the phone's operating system. Conversely, companion apps usually necessitate the registration of a dedicated account. A special case is the Eve app. In our study, the Eve devices, D5 and D6, did not request account registration even when employing their companion app for the onboarding procedure. This "No registration" attribute inherent to these two devices significantly contributed to the streamlining of the otherwise intricate device onboarding process, thereby enhancing the overall user experience.

App permissions request. Either companion apps or platform apps usually ask for several permissions, such as access to contacts, camera, microphone, Bluetooth, location, cloud sync. A companion app may ask permission to connect to a platform app, such as Apple Home, to make the device also available and controllable in the platform app.

4.1.3 Device pairing. Once the app is configured, the app must pair with the new device. Smart-home devices use several different methods for pairing. There are a few elements that compose and influence the pairing process:

Initiated by whom. The pairing process can be initialized by either the user or the device. In the case of user initiation, our study revealed that the user is typically required to manually click the "Add device" button (or something similar) in the app and then select the specific device model. Alternatively, the user-initiated process may entail clicking the "Add device" button, whereby the application autonomously conducts a scan, subsequently presenting information about nearby devices that are prepared for onboarding. In the case of device initiation, the apps typically conduct an automated scan, primarily through Bluetooth, detecting devices that are prepped for onboarding.

Check pairing mode indicator. Some devices require the user to manually check whether the device is in pairing mode, usually by looking at the LED light on the device to see whether it is blinking with a specific sequence of colors.

Onboarding payload retrieval. The app needs to retrieve the onboarding payload, which is composed of important information that is used by the app to ensure interoperability. We saw several onboarding payload retrieval methods: some devices initialized their own temporary Wi-Fi network to pair with the smartphone to exchange information; some exchanged information through Bluetooth; for some devices, the user needed to manually scan the QR code or bar code printed on the device or in its box.

4.1.4 Device configuration. After devices are paired with a smartphone app, they must be initialized. This step often involves connecting to the home Wi-Fi network (for Wi-Fi devices), inputting device information, and updating firmware.

Connect to Home Wi-Fi. Most commercially available smart-home devices require users to connect them to their home Wi-Fi network in the app. Others require the user's assistance to connect them to a Bluetooth or Thread hub.

Input device info. Most devices require the user to name the device and specify the location of the device, whether it is located in the living room, bedroom, kitchen, etc.

Firmware update prompted. Devices that discover new firmware updates may ask to update their firmware.

Once all four steps were accomplished, the device was considered onboarded and part of the home's infrastructure.

4.2 RQ2: Challenges

One key challenge we noticed in our study is that the promised seamless interoperability from Matter is not delivered in reality. Some manufacturers claim their products are compatible with Matter, but their open-box firmware does not actually support Matter. Users must download the companion app and update the device to a Matter-compatible version. For example, when onboarding Aqara Hub M2 through Matter-supported platform apps, the user must perform a firmware update via the Aqara companion app first. This unexpected hurdle disrupts the onboarding process and frustrates users who are expecting a seamless Matter integration.

Another limitation of the use of Matter exists in understanding whether a device requires a Thread Border Router and how the device operates in diverse settings. For example, D9, the Nanoleaf Essentials Smart bulb, does not support Wi-Fi. Without a Thread Border Router, users cannot use the device with platform apps such as Apple Home. While a connection to a phone via Bluetooth using the companion app is possible, it comes with limited functionality Some features, like the schedule feature, are exclusively accessible when connected to a Matter and Thread-compatible smart hub,

i.e., a Thread Border Router. This intricacy may engender user confusion regarding the device's capabilities.

Attempting to connect a device to an unsecured Wi-Fi network without password authentication is often prohibited by smart-home applications, as exemplified in the case of D1. This restriction is anticipated due to the potential exploitation of software or hardware vulnerabilities by users other than the device owner when connected to such networks. Nevertheless, not everyone has access to a secure network, including individuals residing in rented apartments, college dorms, or those dependent on landlord-provided open networks. A solution to this predicament may lie in the adoption of Thread-enabled devices that allow users to build a secure, layered smart-device network atop an open network infrastructure.

4.3 RQ3: Enhancement suggestions

From our results detailed in Section 4, we find Matter plays a key role in enhancing the user experience of smart-home device onboarding, making the onboarding process more uniform and efficient. However, we do not perceive the current Matter protocol as the ultimate solution to smart-device onboarding. Onboarding Matter-compatible devices still requires several manual steps, like scanning QR codes, joining to the device's temporary Wi-Fi to retrieve onboarding payload, and entering home Wi-Fi information or login credentials. These manual steps hinder an efficient and user-friendly onboarding process, especially as the number of devices to be onboarded grows. Therefore, we propose the following enhancements for future systems.

Automatic home Wi-Fi connection. One time sink we observed in our experiments is inputting one's home Wi-Fi credentials to each smart home device that needs to be onboarded. It would greatly enhance users' experiences if the device's connection to one's home network could be automated. To achieve this, the Wi-Fi credentials need to be shared automatically once the device is identified and an authorized user confirms their intention to onboard it. With a centralized system, the user may only need to input their home Wi-Fi credentials once, and the system could store such information under the user's account for future use. As a result, instead of asking the user to input Wi-Fi credentials every time for a new smart-home device, the system only needs to authenticate the user and verify their intention of onboarding before sending the credentials to the device. Many contactless biometric-based user authentication methods that keep users' involvement at a minimum could be used here [5, 6, 13, 17].

Frictionless payload retrieval. As discussed in Section 4.1.3, users must manually scan the QR code or connect to the device's temporary Wi-Fi to retrieve the onboarding payload, which creates another hindrance to users. A more frictionless payload retrieval technology would be desirable. NFC-based payload retrieval could be another solution here, which could be more efficient than connecting to a device's temporary Wi-Fi or scanning a QR code. If we want to improve the efficiency further, a longer-distance device authentication and payload retrieval technique may make the process easier. Instead of asking users to tap each device through NFC, the hub can detect and authenticate multiple devices nearby simultaneously, without the user's involvement. Unfortunately, the trade-off between convenience and security must be considered here. NFC or QR code requires physical proximity or visibility, which prevents nearby adversaries (e.g., your neighbor) from stealthily spoofing ready-to-pair smart-home devices. Longer-distance communication methods may reduce required human involvement at this step, but increase the risk of irrelevant or malicious devices communicating with one's ready-to-pair smart-home device over the air.

Streamline user registration. Eliminating the need for user registration presents another promising direction to streamline the onboarding process. For some devices, one approach is to eliminate the need for an account. In our experiments, devices D5 and D6 do not require account registration, leading to less onboarding complexity and potentially better privacy protection. However, this may be because these devices do not rely on a cloud service and thus do not require a registration – which does not always apply to other devices. For example, D3 stores recorded videos on its own cloud service. Users can only access it by registering an account on their companion apps. Another approach to streamlining the onboarding process is to leverage the user's existing platform account (Apple Home, Google Home, etc.), reducing the time and cognitive burden.

5 LIMITATIONS AND FUTURE WORK

All of our data was collected by one researcher on the team. The researcher had not previously used smart-home devices but self-identified as a technology enthusiast, which can only represent a specific group of smart-home device users. More comprehensive user studies encompassing a broader consumer base or user categories would augment the insights in RQ2 and RQ3.

Moreover, we tested only 12 devices. A follow-up study would include a larger and more diverse array of smart-home devices sourced from various manufacturers. Finally, our methods focused only on device-to-app onboarding, starting from powering the device to the initial device configuration. Integrating the device with other devices or systems (e.g., the home alarm system or the HVAC system) is not in the scope of this paper. Specifically, we did not consider steps like linking smart light switches with light bulbs or integrating smart door and window sensors with the home alarm system. More research on device integration needs to be done.

ACKNOWLEDGMENTS

This paper results from the SPLICE research program, supported by a collaborative award from the National Science Foundation (NSF) SaTC Frontiers program under award number CNS-1955805, and the VeChain Foundation. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors. Any mention of specific companies or products does not imply any endorsement by the authors, by their employers, or by the sponsors.

REFERENCES

[1] Jacob Abbott, Jayati Dev, Donginn Kim, Shakthidhar Gopavaram, Meera Iyer, Shivani Sadam, Shrirang Mare, Tatiana Ringenberg, Vafa Andalibi, and L. Jean Camp. 2022. Privacy Lessons Learnt from Deploying an IoT Ecosystem in the Home. In *Proceedings of the European Symposium on Usable Security (EuroUSEC)*. 98–110. https://doi.org/10.1145/3549015.3554205

[2] Connectivity Standards Alliance. 2023. Matter Core Specification Version 1.1. https://csa-iot.org/all-solutions/matter/
[3] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. 2019. SoK: Security Evaluation of Home-Based IoT Deployments. In *IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, San Francisco, CA, USA, 208–226. https://doi.org/10.1109/SP.2019.00013
[4] Luis Carlos Rubino de Oliveira, Andrew May, Val Mitchell, Mike Coleman, Tom Kane, and Steven Firth. 2015. Pre-Installation Challenges: Classifying Barriers to the Introduction of Smart Home Technology. In *The International Conference on Informatics for Environmental Protection*. 117–125. https://doi.org/10.2991/ict4s-env-15.2015.14
[5] Kailtyn Diederichs, Amy Qiu, and George Shaker. 2017. Wireless biometric individual identification utilizing millimeter waves. *IEEE Sensors Letters* 1, 1 (2017), 1–4. https://doi.org/10.1109/LSENS.2017.2673551
[6] Tianbo Gu, Zheng Fang, Zhicheng Yang, Pengfei Hu, and Prasant Mohapatra. 2019. mmSense: Multi-Person Detection and Identification via mmWave Sensing. In *Proceedings of the 3rd ACM Workshop on Millimeter-wave Networks and Sensing Systems*. 45–50. https://doi.org/10.1145/3349624.3356765
[7] Weijia He, Jesse Martinez, Roshni Padhi, Lefan Zhang, and Blase Ur. 2019. When Smart Devices Are Stupid: Negative Experiences Using Home Smart Devices. In *IEEE Security and Privacy Workshops (SPW)*. 150–155. https://doi.org/10.1109/SPW.2019.00036
[8] Timothy W. Hnat, Vijay Srinivasan, Jiakang Lu, Tamim I. Sookoor, Raymond Dawson, John Stankovic, and Kamin Whitehouse. 2011. The Hitchhiker's Guide to Successful Residential Sensing Deployments. *Proceedings of the ACM Conference on Embedded Networked Sensor Systems* (2011), 232–245. https://doi.org/10.1145/2070942.2070966
[9] Apple Inc. 2023. Home app - The foundation for a smarter home. https://www.apple.com/home-app/
[10] Google Inc. 2023. Smart home automation from Google - Google Home. https://home.google.com/welcome/
[11] Google Inc. 2023. Support device discovery. https://developers.home.google.com/local-home/device-discovery
[12] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(Es) with Smart Home: Experiences of a Living Lab Field Study. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1620–1633. https://doi.org/10.1145/3025453.3025799
[13] Feng Lin, Chen Song, Yan Zhuang, Wenyao Xu, Changzhi Li, and Kui Ren. 2017. Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System. *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking* (2017), 315–328. https://doi.org/10.1145/3117811.3117839
[14] Hui Liu, Changyu Li, Xuancheng Jin, Juanru Li, Yuanyuan Zhang, and Dawu Gu. 2017. Smart Solution, Poor Protection: An Empirical Study of Security and Privacy Issues in Developing and Deploying Smart Home Devices. In *Proceedings of the Workshop on Internet of Things Security and Privacy (IoTS&P)*. 13–18. https://doi.org/10.1145/3139937.3139948
[15] 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 International Workshop on Mobile Computing Systems and Applications (HotMobile)*. 117–122. https://doi.org/10.1145/3301293.3302371
[16] Sarah Mennicken and Elaine M. Huang. 2012. Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them. In *Pervasive Computing (Lecture Notes in Computer Science)*, Judy Kay, Paul Lukowicz, Hideyuki Tokuda, Patrick Olivier, and Antonio Krüger (Eds.). 143–160. https://doi.org/10.1007/978-3-642-31205-2_10
[17] Lei Wang, Kang Huang, Chen Tian, Ke Sun, Wei Wang, Lei Xie, and Qing Gu. 2018. Unlock with Your Heart: Heartbeat-based Authentication on Commercial Mobile Phones. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol* 2, 140 (2018), 22. https://doi.org/10.1145/3264950
[18] Jong-bum Woo and Youn-kyung Lim. 2015. User experience in do-it-yourself-style smart homes. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '15*. ACM Press, New York, New York, USA, 779–790. https://doi.org/10.1145/2750858.2806063
[19] Nan Zhang, Soteris Demetriou, Xianghang Mi, Wenrui Diao, Kan Yuan, Peiyuan Zong, Feng Qian, XiaoFeng Wang, Kai Chen, Yuan Tian, et al. 2017. Understanding IoT security through the data crystal ball: Where we are now and where we are going to be. *ArXiv preprint* (2017). https://doi.org/10.48550/arXiv.1703.09809
[20] Wei Zhou, Yan Jia, Yao Yao, Lipeng Zhu, Le Guan, Yuhang Mao, Peng Liu, and Yuqing Zhang. 2019. Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms. In *Proceedings of the USENIX Security Symposium*. 1133–1150. https://doi.org/10.5555/3361338.3361417