Understanding user perceptions of privacy, and configuration challenges in home automation

Kim J. Kaaz, Alex Hoffer, Mahsa Saeidi, Anita Sarma and Rakesh B. Bobba
School of Electrical Engineering and Computer Science
Oregon State University, Corvallis OR, USA

***Abstract*—Home automation has become increasingly popular, with new interconnected products being introduced on a regular basis. While the benefits of these devices are tantalizing, end users may not fully understand the complexities of setting up these devices, become frustrated with the process, or have incorrect installations. We performed an exploratory study to understand the barriers that they face in actually setting up these devices. Participants faced multiple barriers, some of which were insurmountable. Our work indicates that current home automation devices run contrary to the perception that smart homes devices are "plug-and-play".**

***Index Terms*—Home automation, Internet-of-Things (IoT), configuration barriers, mental model gaps**

I. Introduction

We are now in the midst of a technology wave dubbed the *Internet-of-Things (IoT)*. Since Smartphones became mainstream about a decade ago with the arrival of the iPhone, the number of smart and connected devices (*e.g.,* tablet computers, e-readers, smartwatches, health monitoring devices, voice-controlled devices *etc.*) has increased significantly.

This IoT technology wave is accelerating the proliferation of connected devices in homes. Smart door locks, thermostats, lights and switches that can be operated remotely using smartphones are just a few examples of popular smart home devices. Gartner predicts that future smart homes could have 500 or more smart and connected devices [2]. In another recent report, Gartner forecast that the number of connected things will increase to 20.4 billion by 2020 from the 8.4 billion in 2017, with total spending reaching 2 trillion [4]. While these numbers include all connected things, the consumer segment alone makes up 63% of the total.

So what drives this demand? A survey in 2015 by iControl [1], a software platform provider for major home automation companies (*e.g.,* ADT, XFINITY, AT&T), found that *personal and family security* are the primary drivers, closely followed by excitement about energy savings [3].

While home automation solutions have been around for some time, currently there is a proliferation of self-installed home automation and monitoring kits (*e.g.,* SmartThings, Iris, Piper, Insteon, Wink *etc.*) and apps (*e.g.,* HomeKit). To make it easier for end users to configure devices, many vendors are embracing the *ZeroConf* or *Plug'n'Play* [5] philosophy. Zeroconf and plug-and-play refers to technologies that automatically create a usable network without manual configuration.

In this context, we need to understand what people know and do not know when configuring smart devices for two reasons. First, understanding how end-users think that their devices operate will help us identify the gaps in their security and privacy perceptions, and the potential points of failure because of misconceptions. Second, understanding where end users face barriers because they do not understand how to correctly set up devices will help us create awareness among manufacturers about the need to improve the installation process and the need for better documentation regarding privacy and security implications.

II. Background and Related Work

Barriers to Configuration: In our study, barriers refer to the issues end users have when configuring home automation devices. Barriers in computing are not new, for instance, prior research has focused on barriers in software development [8], [12] and to adoption of home automation technology [6]. Barriers that developers face have been classified as either surmountable or insurmountable [8]. As the name indicates, surmountable barriers are those that were eventually overcome, while insurmountable ones are those that couldn't be. We leverage this notion of barriers to articulate the configuration problems that participants in our study faced.

Ko *et al.* [12] identified six barriers in developing software, namely, design, selection, coordination, use, understanding, and information. In our case, the use barrier is the most pertinent, since users may have trouble configuring and using a home automation device. Brush *et al.* [6] identified four barriers to adoption of home automation technology, namely, cost, technology flexibility (or interoperability), poor manageability, and security concerns. Barriers related to poor manageability and security concerns of home automation are closely related to this work. However, since the work of Brush *et al.* [6], home automation technology has undergone tremendous changes with the emergence of IoT, and the proliferation of smart phones and tablets that are used in configuring and controlling home automation devices. Our work focuses on barriers to configuring and setting up newer home automation devices that essentially claim to be plug-n-play.

Mental models: are a commonly used methodology in psychology to elicit users' understanding about a problem or

This work is partly supported by NSF: IIS-1559657 and CCF-1560526.

TABLE I: Background of participants

P#	Gender	Prior IoT experience	Home network setup	Online banking
P1	F	No	Yes	Yes
P2	F	Yes	Yes	Yes
P3	F	No	Yes	Yes
P4	M	Yes	Yes	Yes
P5	M	No	No	Yes
P6	M	No	No	Yes
P7	M	No	Yes	Yes

systems. Mental models have been adopted by researchers to study users' understanding of both security and privacy threats, and technologies (*e.g.,* [9], [13], [15], [16]). Our work aims to understand the mental models (and gaps) that end users may have when installing, configuring, and managing emerging smart home-automation devices; and the associated security and privacy concerns.

III. Methodology

We conducted a user study to investigate how our target population configured home automation devices. Specifically, we were interested in evaluating the usability of these devices, their security and privacy configurations, and whether end users understood the security and privacy implications of their configurations. Our target population was working individuals 18 or older who were homeowners, because this population is likely the most typical consumer of smart home devices.

Device description. We selected the following 6 devices that participants configured.

- **Amazon Echo**: is a voice controlled assistant.
- **Insteon Hub**: connects to a family of smart devices and allows users to control them through an app.
- **Nest Camera**: captures a video feed.
- **Phillips Hue Lights**: remotely turn lights on and off.
- **Belkin WeMo Switch**: enables remote control of an electrical outlet.
- **Kwikset Kevo Smart Lock**: a smart door lock that can be controlled with a mobile device.

Recruitment process. We recruited 7 participants: three female and four males; all within the age range of 35 to 64 (See Table I). A sample of 7 participants was chosen to ensure that each device would be configured at least 3 times. None had a computer science background.

Study process. The study was conducted in an IoT lab at Oregon State University. Participants were first asked to provide background information about their prior IoT experience, setting up networks, and on-line banking. Then, the participant was asked a series of 5 questions. These questions were concerned with what the user thought the device did and how data related to the device was controlled and used. Additionally, they were asked to draw a diagram that indicated how data flowed between the app and the smart device in any form they choose. Diagramming in addition to verbal answers is a helpful tool to elicit mental models [10] and has been used by others (*e.g.,* [11], [14]).

Device configuration. After the initial set of questions, the device was given to the participant in its box, reset to factory settings. They were allowed to choose between a provided Apple or Android tablet to install the device's app on. Participants then configured the device without assistance.

IV. Results

We investigated three aspects in our exploratory study. First, we identified the barriers faced by participants when configuring the devices (IV-A). Barriers in correctly installing the device can lead to frustrations, and more importantly incorrect installations that might have security and privacy implications. Second, we find whether there are gaps in end users' expectations of the devices and how these devices manage their data (IV-B). A gap in an understanding how the device data can be accessed by others can lead to security/ privacy concerns. Finally, we analyze the change in participants' trust levels before and after they installed the device.

A. Barriers they face in actually setting up these devices

Most participants faced barriers when they configured the devices. These barriers were in: (1) finding the right app from the App Store, (2) setting up the network, and (3) following the instructions provided in the device packaging.

Tables II and III show the number of steps that participants needed to configure each device. Green check marks indicate that participants were successful in the particular step, red triangle marks indicate a barrier that the participant was able to surmount, red stop sign indicates that the participant encountered an insurmountable barrier and stopped, and hollow black circles indicate steps that participants did not attempt either because they ran out of time or unwilling to go further. Dash in a cell is used to indicate that the participant did not configure that device. Note that despite Hue Light being a simple device, three (P1, P2, P5) out of the five participants failed to configure the device. The Nest Camera and Amazon Echo also had many barriers, which we discuss next.

Finding the right app. The most significant barrier was right in the first step – installing the app. Instructions provided in the device package asked participants to download the requisite app from from the App Store, but did not account for the presence of "imposter" apps or the app being missing in the App Store. For example, a search on "Hue Lights" provides the following apps (see Figure 1). The first and many subsequent apps are third-party software for controlling Hue Lights. The second and fourth apps are Philips Hue, but one is from "Philips Lighting BV" and the other from "Philips Consumer Lifestyle". Similar problems existed for other devices including Nest camera.

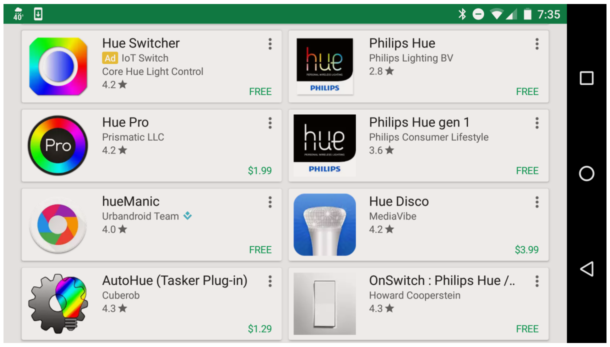
While "finding the right app" might be a simple problem of identifying the correct app in the App Store, it has deeper security implications. Installing a fake app can lead to a user's smart phone being hacked or data theft. This was especially true for the Kevo Lock and WeMo Switch. No apps could be found in the App Store through a search. As a result, P1 and P6 incorrectly installed the wrong Kevo app by Kwikset, the parent company of Kevo. After the app didn't work with the Kevo, P1 and P6 searched the web for the right app and successfully installed it.

TABLE II: Displays the steps and how far each participant went before hitting a barrier for the Hue, Nest, and Insteon

P#	Hue	Nest	Insteon
P1	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ △ ✓ ✓ ✓ ✓ ●	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ △ ✓ ✓ △ ●○ ○ ○ ○ ○ ○ ○ ○ ○ ○	–
P2	✓ ✓ ✓ △ ✓ ✓ △ ✓ ✓ ✓ ✓ ✓ ✓ △ ✓ ✓ ✓ ●○	–	–
P3	–	✓ △ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ △ ✓ ✓ △ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	✓ ✓ ✓ △
P4	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	–	✓ ✓ ✓ △
P5	✓ △ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ●	–	–
P6	–	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ○ ○ ○ ○ ○ ○ ○ ○ ○	✓ ✓ ✓ △
P7	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ △ ✓ ✓ ✓ ✓ ✓	–	–

TABLE III: Displays the steps and how far each participant went before hitting a barrier for the Kevo, Echo, and WeMo

P#	Kevo	Echo	WeMo
P1	△ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ △ ✓ ✓ ✓ ✓ ✓ ✓ ✓	–	–
P2	–	✓ △ ✓ △ ✓ △ ✓ ●○ ○ ○ ○ ○ ○	✓ ●○ ○ ○ ○ ○ ○ ○ ○
P3	–	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	✓ △ ✓ ✓ ✓ ✓ ✓ ✓ ○ ○
P4	△ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ○ ○ ○ ○ ○ ○ ○	–	–
P5	–	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ △ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ○ ○
P6	△ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ △ ✓ ✓ ✓ ✓ ✓ ✓	–	–
P7	–	✓ △ ✓ ✓ ✓ ✓ ✓ ●○ ○ ○ ○ ○ ○	–



7:35

Hue Switcher
Ad IoT Switch
Core Hue Light Control
4.2 ★
FREE

Philips Hue
Philips Lighting BV
2.8 ★
FREE

Hue Pro
Prismatic LLC
4.2 ★
$1.99

Philips Hue gen 1
Philips Consumer Lifestyle
3.6 ★
FREE

hueManic
Urbandroid Team
4.0 ★
FREE

Hue Disco
MediaVibe
4.2 ★
$3.99

AutoHue (Tasker Plug-in)
Cuberob
4.3 ★
$1.29

OnSwitch : Philips Hue /..
Howard Cooperstein
4.3 ★
FREE

Fig. 1: List of apps displayed for a search on "Hue Lights"

Following instructions. Typical instructions provided in the pamphlet were deceptively simple, consisting of just two steps: plug-in the device and install the app. The instructions implied that the installation process is trivial. However, the opposite is true. In Table II and Table III, each of the symbols (checkmark, triangle, stop-sign and hollow circle) represents one step in the installation process required to set up a device. There are 24 steps needed for the Nest Camera, and a minimum of 11 for the WeMo Switch. Such a vast discrepancy between the 2-step process implied by the instructions and the actual number of steps was a problem since participants started with a mindset that the process was going to be simple, and then were frustrated with the total number of steps that were actually required. P1 kept exclaiming the "*the directions are bad*" when setting up the Amazon Echo and WeMo Switch devices.

Setting up the network. The Nest Camera and Amazon Echo had the most barriers (see Tables II and III). In the case of the Nest Camera, two out of the three participants faced barriers. For P1, the network failed three times when trying to configure, since she did not input the password for the network. However, this step was not made clear by the app, which provided no authentication prompts. Because of the Zero-Conf configuration style of Nest Camera, participants were not asked to input the password directly into the app. Instead it required them to move back and forth between screens in the app to do so. This caused confusion and added to the cognitive load of setting up the device. P3 had similar issues and gave up configuring the device after 4 attempts.

Types of barriers. We classified a barrier as surmountable when the participants could overcome the barrier within the study time frame. Whereas, those barriers that participants could not overcome are classified as insurmountable.

The usability of the apps was a common *surmountable* barrier. The most common failure was when participants set up the Hue Light timer or light on/off feature. Participants were not able to save the new rule and got an error in the app. The app provided a warning popup asking the participant to use help, which can be a great example of providing contextualized help [7]. Unfortunately, there was no help feature available in the app, which only frustrated the participants further and reduced their trust in the device.

A key *insurmountable* barrier was that the Kevo Lock was incompatible with both our Android (study) tablet as well as the participant's Android phone. We verified that we had the right version of the OS. In this case, the participant could not install the device at all (and was forced to use an iPad, a device with which they were unfamiliar).

B. Gaps in mental-model

There were differences in the mental models (or mental model gaps) generated by participants about how a device operated, stored, or used the data and the reality. Although, many of the participants were new to IoT, they all used a wireless network at home and possessed smart phones. However, despite the everyday use of smart phones, a majority of participants had gaps in their understanding of the complexity of the devices. Mental model gaps existed across all devices, and across the five questions about the device use and its data access. This shows that understanding how IoT home automation devices operate is nontrivial.

To better understand mental model gaps, let us consider Hue Lights, which is a device that should have been relatively easy to understand and set up. However, every participant had gaps in their mental model about the device. An example of a gap is demonstrated by participant P1 (in Figure 2a), where she thought that the iPad communicated directly with the light bulb. After installing the device P1 understood more about the dataflow, as she realized that the Hue Bridge communicated with the light bulb. However, she still had an incorrect mental model of where the data is stored (Figure 2b).

Most of the gaps continued to be in the use and control of data collected by the devices, as participants expected their data to be private and not accessible to third party vendors.

C. Trust in Devices

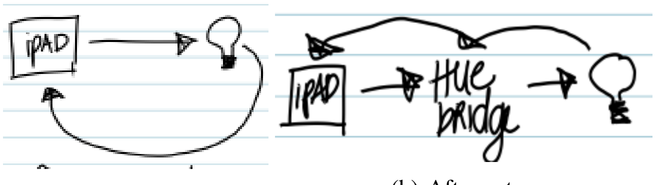
We present here the difference in trust levels before and after participants installed devices. We specifically did not define trust when asking this question of the participants, as our main goal was to understand whether participants would trust the device enough to use it in their homes. Participants answered using a Likert scale 1-5, with 1 indicating strong trust and 5 indicating strong distrust. Figure 3 shows the change in trust level after installation. Left of the line, in red, shows decrease in trust levels, while to right of the line, in green, displays increase in level. In only one case, Participant P6, increased his trust on the Kevo Lock. P6 said that he increased his trust level: "*...because it had security and password privacy*".

In all other cases, the trust levels either stayed the same or decreased, with the worst evaluation being of Hue lights. Reasons for lowering in trust levels ranged from getting a better understanding of the functionality of the device after installation, to the barriers faced when setting up the device.

V. Discussion

We discuss the implications of the barriers here.

Lack of Options: Despite security and privacy concerns, the current state of Home Automation does not allow for these devices to have a wide variety of configuration or storage options for users to choose from. Our original goal was to understand the issues that end users might face in configuring these devices. However, we found that most smart home devices employ Zero-Conf inspired configuration processes. In doing so, they force end users to accept the vendor's concept of security, minimizing users' opportunities to secure their own devices [5]. Additionally, there is no easy way to understand the implications of the use of the device, because of which users may not understand the security and privacy implications behind how these devices store and transfer data.



(a) Before setup (b) After setup

Fig. 2: P1's drawing of Hue Light communications

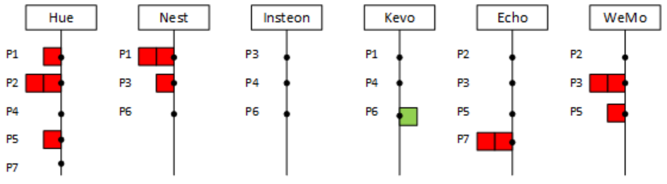


Fig. 3: Participants' differences in trust levels after installation.

Incorrect expectations: Homeowners expect privacy and security in their home, the old idiom "*My house is my castle*" simply means others have no right to enter without the householder's permission. However, with devices such as Amazon Echo anyone who is within range can give voice commands. For example, we were able to activate and give Amazon Echo instructions from outside the office where it was situated (behind a wall). This suggests that malicious users can take control over the smart devices within the users' home.

Given that security and privacy were cited as the main reason why participants would use home-automation devices, this is an important concern. The largest mental model gap in our study showed participants did not expect others to use their data. Had they read the privacy statement first, their expectations might have been different. Only one participant read the privacy notice, where companies state what private data is collected and who it is shared with.

Limitations and future work: We specifically recruited older participants from non-technical education backgrounds, as we wanted to understand the mental models of end users who are used to smart phones, and have sufficient purchasing power. Furthermore, being an exploratory study, we had a small pool of participants. The small sample size and our demographics choice may affect the types of mental model gaps and barriers that participants' faced. As future work, we plan to replicate the study with participants who are in the tech-field, as well as participants who are younger. It is possible that there is an interplay between demographic factors and users' mental model of device operations and data management. Another limitation is that we time-boxed each device installation to 20 minutes to accommodate at least three devices per participant. It is possible that some participants could not complete the installation because of this constraint. It would be interesting to study how participants' trust levels and completion rates change with different installation time bounds.

VI. Conclusion

Growth of home automation depends not only on manufacturers creating new and exciting devices, but also on homeowners' ability to successfully incorporate them into their lives. Homeowners need to evaluate the benefits provided by home automations versus the privacy and security threats. But to do so, they need to be able to comprehend how the devices actually operate and the risks associated with them.

Many of the barriers that participants faced could be solved through better directions and examples of configuration settings. In fact, the false impression given by the devices as simple "plug and play" might have caused a mismatch in participants' expectations, which in turn caused them to be frustrated, and/or reduce their trust scores.

Our work suggests a need for further study to understand better the privacy and security concerns with home automation devices from the perspective of installing and using such devices by everyday end users.

REFERENCES

[1] www.icontrol.com.

[2] The Future of Smart Home: 500 Smart Objects Will Enable New Business Opportnities. http://www.gartner.com/newsroom/id/2839717, September 2014.

[3] 2015 STATE OF THE SMART HOME REPORT. https://www.icontrol.com/blog/2015-state-of-the-smart-home-report/, 2015.

[4] Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. http://www.gartner.com/newsroom/id/3598917, February 2017.

[5] X. Bai, L. Xing, N. Zhang, X. Wang, X. Liao, T. Li, and S. M. Hu. Staying secure and unprepared: Understanding and mitigating the security risks of apple zeroconf. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 655–674, May 2016.

[6] A. B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon. Home automation in the wild: Challenges and opportunities. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2115–2124, New York, NY, USA, 2011. ACM.

[7] J. Cao, S. D. Fleming, M. Burnett, and C. Scaffidi. Idea garden: Situated support for problem solving by end-user programmers†. *Interacting with Computers*, 27(6):640, 2015.

[8] J. Carter, P. Dewan, and M. Pichiliani. Towards incremental separation of surmountable and insurmountable programming difficulties. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, SIGCSE '15, pages 241–246, New York, NY, USA, 2015. ACM.

[9] B. Friedman, D. Hurley, D. C. Howe, H. Nissenbaum, and E. Felten. Users' conceptions of risks and harms on the web: A comparative study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '02, pages 614–615, New York, NY, USA, 2002. ACM.

[10] D. Jonassen and Y. H. Cho. Externalizing mental models with mindtools. In *Understanding models for learning and instruction*, pages 145–159. Springer, 2008.

[11] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, 2015. USENIX Association.

[12] A. J. Ko, B. A. Myers, and H. H. Aung. Six learning barriers in end-user programming systems. In *Proceedings of the 2004 IEEE Symposium on Visual Languages - Human Centric Computing*, VLHCC '04, pages 199–206, Washington, DC, USA, 2004. IEEE Computer Society.

[13] M. L. Mazurek, J. P. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon, R. Shay, K. Vaniea, L. Bauer, L. F. Cranor, G. R. Ganger, and M. K. Reiter. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 645–654, New York, NY, USA, 2010. ACM.

[14] E. S. Poole, M. Chetty, R. E. Grinter, and W. K. Edwards. More than meets the eye: Transforming the user experience of home network management. In *Proceedings of the 7th ACM conference on Designing interactive systems*, DIS '08, pages 455 – 464. ACM, ACM, 2008/// 2008.

[15] F. Raja, K. Hawkey, and K. Beznosov. Revealing hidden context: Improving mental models of personal firewall users. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, pages 1:1–1:12, New York, NY, USA, 2009. ACM.

[16] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 11:1–11:16, New York, NY, USA, 2010. ACM.