When Smart Devices Are Stupid: Negative Experiences Using Home Smart Devices

Weijia He, Jesse Martinez, Roshni Padhi, Lefan Zhang, Blase Ur
University of Chicago
{hewj, jessjmart, padhi, lefanz, blase}@uchicago.edu

***Abstract*—Household smart devices – internet-connected thermostats, lights, door locks, and more – have increased greatly in popularity. These devices provide convenience, yet can introduce issues related to safety, security, and usability. To better understand device owners' recent negative experiences with widely deployed smart devices and how those experiences impact the ability to provide a safe environment for users, we conducted an online, survey-based study of 72 participants who have smart devices in their own home. Participants reported struggling to diagnose and recover from power outages and network failures, misattributing some events to hacking. For devices featuring built-in learning, participants reported difficulty avoiding false alarms, communicating complex schedules, and resolving conflicting preferences. Finally, while many smart devices support end-user programming, participants reported fears of breaking the system by writing their own programs. To address these negative experiences, we propose a research agenda for improving the transparency of smart devices.**

***Index Terms*—Smart homes, Security, Safety, IoT, Bugs**

I. Introduction

Currently, 32 % of U.S. households have at least one internet-connected smart device, and this figure is expected to rise to 53.1 % of U.S. households by 2022 [1]. Popular internet-connected smart devices include thermostats, lights, cameras, door locks, voice assistants, and more. This wide deployment makes "smart homes" not just a concept in research or fiction, but a reality of daily life.

Home smart devices can provide convenience, improve customizability, and dynamically conserve resources [2]. However, errors and failures in any system can cause frustrations and user friction. There is a small body of prior work suggesting challenges users might face in smart homes [2], [3], [4], [5]. However, the rapid deployment of current smart devices provides an excellent opportunity to look into users' actual negative experiences using common smart devices, comparing them with those anticipated by the literature.

To understand users' recent real-world experiences with smart devices, especially negative experiences, we conducted an online, survey-based study of 72 participants who had at least one smart device in their own home. We asked about their and their friends' household smart devices, focusing on experiences related to power and network failures, built-in learning, and writing custom rules.

Participants reported misattributing a loss of connection to their home being hacked, and they worried about how to properly diagnose related events in the future. For devices with built-in learning features (e.g., the Nest learning thermostat), participants reported difficulties regarding complex schedules and cases where household members had conflicting preferences. For devices with built-in motion detection or entity recognition, they reported frustrations related to frequent false alarms. Finally, while many smart devices support end-user programming, participants reported fears of breaking the system by writing their own programs. Some of the experiences participants reported are best classified as usability issues, but others directly impact the security and safety of the home. Beyond adding to the literature the latest usage problems with smart devices, we propose a research agenda for enhancing the transparency of smart devices in order to minimize these negative experiences and better equip users to correctly diagnose abnormalities in their smart devices.

II. Related Work

As household smart devices have become ubiquitous, researchers have examined the evolving definition of a "smart home" [2], [6], emphasizing opportunities for automation. However, many aspects of the smart device user experience can go wrong. Prior work has documented device configuration to be taxing [3], [7]. Transparency regarding device behavior is sorely lacking when it comes to household routines [2], [3], [8], [9]. Users are frustrated by their inability to communicate their intent to the Nest thermostat [8]. They can also be frustrated by smart devices rendering the home impersonal [2], [6] or exacerbating conflicting preferences among household members [4], [10].

Security and privacy concerns can also contribute to negative experiences. These threats are both external (the Mirai botnet exploited smart cameras) and internal (snooping by household members). Qualitative work found many users have incomplete mental models of these threats [11]. Users struggle to configure nuanced access controls for smart devices [12]. Furthermore, tech-savvy device administrators can exclude other household members [2], [9], [11]. Smart devices also enable surveillance of teenagers [13] and intimate partners [14]. On the horizon, new attacks like skill-squatting on voice assistants [15], [16] will make the IoT security landscape even more complex.

End-user programming empowers users to automate smart devices [17], [18]. It also introduces frustrations [7]. Some desired behaviors are difficult to express with common interfaces [19]. Subtle programming errors create mismatches

between expectations and reality [20], [21], and debugging is often challenging [7], [22]. Research on supporting debugging for end-user programs focuses on visualizing events in the home [9], [23]. Efforts to improve program correctness have enabled rule creation through crowdsourcing [24] and synthesis from natural language [25], [26], [27], [28].

A number of efforts aim to improve safety, security, privacy, and correctness for smart devices. Some efforts employ formal methods [29], [30], [31], [32], while others use information flow control [33], [34], [35], [36], [37]. Yet others seek to redesign systems to minimize overprivilege [38], [39].

III. Methodology

We conducted an online, two-part survey of current users of smart devices in July 2018. The first part of the survey was designed to understand device owners' frustrations and negative experiences with smart devices. The second part elicited potential invariants about the state of the house. In this paper, we report on only the first part of the survey. The results of the second part have been reported separately [32].

We recruited participants on Mechanical Turk, requiring that they own at least one smart device. We defined smart devices as "Internet-connected lights, thermostats, cooking devices, locks, outdoor equipment, and cameras" in our recruitment. We excluded voice assistants, computers, smartphones, and tablets from this definition because they are not actuators and not controllable in the same manner as other smart devices. Our IRB-approved survey took roughly 30 minutes to complete. Participants were compensated $5.00 USD.

A. Study Protocol

We presented participants with a list of internet-connected devices and asked them to select all devices they had used, writing any brand names they could recall. We then asked about their experiences and anticipated frustrations with these devices in four sections. Each section focused on a topic: network and power failures; built-in features; rules and end-user programming; and other experiences.

For each section, we provided definitions shown to be necessary in pre-study piloting. We asked whether the participant recalled any frustrating experiences related to the topic. If so, they described their experiences in free text. If not, we asked if anyone they knew had reported such frustrations, describing the reports in free text. Participants who answered no to both described frustrations they had anticipated having. We ended with demographics questions.

B. Analysis

We performed open coding and axial coding, creating a codebook for each of the four survey sections [40]. Our codebook covered a range of reported problems, including device non-responsiveness, opaque behavior, and security fears. Two coders used this codebook to independently code all responses, with an average Cohen's κ of 0.71 across sections. The coders met and resolved disagreements.

C. Limitations

A convenience sample of participants self-reported their past experiences, which limits both the generalizability and accuracy of their reports. Furthermore, because of the highly structured survey questions that we found in pilot testing to help participants recall their prior experiences, responses tended to center on experiences related to power outages, network failures, learning features gone wrong, and writing automation rules. Although the last section solicited additional frustrations broadly, few participants reported others.

IV. Results

We recruited 75 participants, discarding the incomplete or off-topic responses from three participants. The remaining 72 participants are our sample. Our sample skewed young, with 75 % of participants between 18 and 34. Among participants, 63.9 % identified as male and 36.1 % as female. 55.6 % reported holding a bachelor's degree or higher, and 23.6 % stated they held a degree or job in computer science or a related field.

Of the 72 participants, 70 permitted the release of their anonymized responses. These responses are available online.[1]

All participants reported owning smart devices. Most had only a few smart devices; 75 % reported owning only one or two types of smart devices. Participants most frequently owned internet-connected cameras (55%), lights (54%), thermostats (52%), cooking devices (18%), and door locks (15%). 95 specific products from both major manufacturers (e.g. Nest, Phillips) and smaller companies (e.g. Night Owl) were mentioned by 55 participants. We did not observe a significant correlation between the popularity of the company and the number of complaints participants reported ($p = 0.343$).

A. Network Failure and Power Outage

Of our participants, 34.7 % (n = 25) reported that they had had frustrating experiences with smart devices because of a network failure or power outage. Connection failures were the most frequently mentioned frustration overall. Of these 25 participants, however, only 9 listed device unresponsiveness as the sole reason for frustration.

Losing connection to a security-related device can be upsetting. Three participants reported cases where device owners were especially upset when this occurred while they were on vacation. The service interruption led people to think intruders were in the house, or that their cameras had been hacked. One participant wrote, "My sister in law was out of town when she called to ask if I could go check on the house because her outdoor cameras had shut off. There was a power outage in her area that knocked everything out. She wasn't aware of the outage until I got there and called to let her know. She thought someone had done something to her cameras because she didn't get any notifications or anything." Another participant said losing the connection to his camera made him feel "a loss of security."

[1] https://github.com/UChicagoSUPERgroup/safethings_2019

Users cannot tell the difference between a network or power failure and an intentional disconnection by an intruder, which is problematic given how common such events can be. For example, one participant wrote, "Living in Florida, we have almost daily afternoon thunderstorms and we lose power almost every time." Users may not only misattribute natural failures of the system to hacking, but may also believe an actual intrusion is just another power or network failure.

Nine participants mentioned that they could not diagnose why their devices were not connected to the internet. One participant searched for help online, but could not resolve the issue and eventually stopped caring. He said, "I tried changing my router to see if it would improve stability at the advice of some online articles but it didn't help. I couldn't find a solution for the issue and just kind of stopped caring."

Participants frequently mentioned the inconvenience of resetting the device when it reconnected. One participant wrote, "My internet stops working at random times and the camera has to be reset." However, resetting the device meant users had to reconfigure it, a tedious task. Another participant noted, "Every time [a network failure] happens, you have to reconnect [smart light bulbs] and at that point, it's more effort to go through that than it is to get up and work the switch yourself."

Moreover, some smart devices lost all settings after even a simple restart. One participant reported, "About a month ago I lost power for 45 minutes. When my power came back on my ecobee4 thermostat was acting up. I had to reprogram the entire thing to have it functioning properly again."

B. Error-Prone Built-In Features

Many smart devices possess features that try and make the devices "intelligent." Among these are environmental detection (e.g. motion, temperature, contact) and preference learning. Unfortunately, these techniques are error-prone and at the root of many users' frustrations.

Some participants complained their security cameras detected motion when there was none. One participant wrote, "It's annoying to me because I get nervous at first that something is in the room when there wasn't at all."

Participants also reported that cameras have difficulty distinguishing between human and non-human activities. For example, "Motion detection either doesn't work at all or sees things that one generally would not be concerned with... such as pets." Another participant wrote, "Cameras that were supposed to activate when motion is detected, activated every time the wind blew." Frequent false alarms can cause habituation, which may lead to negligence towards suspicious activities and render the alarms ineffective.

Besides false detection, participants complained about struggling with the learning modules in smart thermostats. One wrote, "I tried to have the Nest do that learning thing but our schedules are so crazy I think it couldn't adapt." Preference conflicts between family members also cause trouble: "Our Nest thermostat is set up to learn our preferences. But my husband's preference is to keep the house like a fridge and my preference is to be able to afford to pay for our electricity. So, I am constantly having to change the 'learned' preferences to keep our electricity usage within our budget."

One participant also reported smart thermostats' learning to be overly sensitive to frequent temperature adjustments. He wrote, "A friend of mine's family likes to mess with their smart thermostat rather often... The thermostat is changing the house temperature because it is trying to read a pattern or preference that he says doesn't exist."

These concerns open up an attack vector where an internal attacker can leverage the sensitivity of the learning algorithms to change users' settings for their own benefits. Although messing with thermostat readings seems harmless, one could imagine how the situation could spiral in future smart homes, where machine learning is deployed to more security-critical devices, or attackers escalate their access by exploiting user-specified trigger-action rules.

C. Rule-Creation and Program-Writing

Among participants, 82 % ($n = 59$) reported they had *never* written automation rules or end-user programs to control their smart devices. The most common reason ($n = 32$) was that they had no experience in programming and thought it would be burdensome to learn. Exemplifying this belief, one participant wrote, "I have no experience in writing programs/code so it will be a relatively high learning curve." Because of their inexperience, some worried that their code would break the system. "I mostly just do whatever is automatic for the system. I'd be afraid that I'd break something if I tried to write my own. I feel like I don't know enough," one stated.

Some participants also believed one had to be an expert to write rules and programs. For instance, "I think high programming skills is required to write the code to control internet connected household devices. [You need to] clearly know the hardware parts to write code." With end-user programming, however, this is untrue [17], [18]. Even if participants knew there was an easy way to program devices, their responses indicated they would still worry their rules would sometimes fail. One participant wrote in the response, "I do not know how to write code so this is not something that I would do. If I could write code I would think that it would do something other than what I wanted it to do."

Among participants, 9.7 % ($n = 7$) reported that they had written individual automation rules before, but had never written more complex programs. Of these seven, none reported difficulties writing rules even though three had no technical experience. It appeared writing automation rules did not challenge experienced users, but inexperienced users were intimidated by the system. Fortunately, all participants reported accomplishing their goals when writing rules. One participant was even successful in debugging his code. He wrote, "I followed a tutorial online that would help me send important footage to my Dropbox but it only worked half the time. When the file failed to send because of low bandwidth like when someone else in the house is streaming something or playing video games, it wouldn't attempt to send again. I fixed it

including a rule to check on my Dropbox to see if the file was confirmed to be sent."

Though all of these participants reported success writing rules, a few had complaints. One participant thought current end-user programming platforms like IFTTT [41] were too limited to express the behaviors she desired. She wrote, "I tried to use IFTTT to start the Roomba under certain values, but the if and thens I wanted to set up were too complicated for the app." Responses also did not note any instances of apps or devices intervening to notify users of mistakes. Future interfaces should proactively notify users about potential bugs.

V. Discussion

In the previous section, we saw the frustrations that end users encountered when using household smart devices. While some issues simply distress users, others can seriously impact the security of one's home. In this section, we propose a research agenda aimed at minimizing the negative experiences our participants reported.

A. Handling Network and Power Failures

a) Notifying Users Who Are Away: Current household smart devices do not provide enough information to users when a network or power failure occurs. As discussed in Section IV, without properly notifying users about the causes of failures, users cannot differentiate between natural failures and suspicious activities, which results in distress while also crying wolf, deteriorating their ability to be vigilant towards possible future malicious attacks.

Systems should proactively inform users when network or power failures are the source of a lost connection. Most smart devices have two-way communication with cloud servers. Servers should thus be able to detect sudden connection losses and diagnose the root cause through judicious testing. Devices and smart hubs with access to cellular networks and backup batteries can keep guarding the house and report to servers about the activation of backup network and power systems.

For regional outages, online reporting systems could corroborate outages. Manufacturers of widely used devices could also detect geographic failure trends themselves. If the cloud server confirms a house was affected by a regional outage, members of the household should be proactively notified.

b) Recovery: Another common result of outages and failures was inappropriate device behavior on reboot. Some users were upset their devices had to be manually reconfigured. Others did not want devices to return to their last state prior to the failure, which was often contextually incorrect.

The system ought to determine if a given device's state should have changed while it was offline. For example, consider a power outage beginning at 7:00 pm and ending at 1:00 am. A smart lamp might have been on prior to the outage, but should be off upon reset since it could disturb sleeping household members. However, if the AC was on before a power outage, the user might want it to turn on again when the outage ends. A possible solution is to let users set a custom *recovery state* for devices. When a device regains service, it would enter that recovery state, not its pre-outage state.

Instead, if a user manages their home with automation rules, nuanced and appropriate recovery states could be specified through user-written rules. For example, if the rule "turn the lights off at 10:00pm" was active, the recovering system in the example above could determine the lights should have turned off during the outage, subsequently keeping the lights off. Complexity increases, however, with larger rule sets.

State calculation and coordination could still take place when connection to the wider Internet is lost. However, this requires either a localized, in-home hub or mesh networking between devices, departing from the network models widely deployed for today's smart devices.

B. Leveraging Collective Information

We found that false alarms and sensor misreadings can make devices unusable and annoy users. One solution is to combine information from different sources. There is research about secure state estimation, in which the researchers tried to reconstruct system states when a subset of sensor readings were tampered with by attackers [42], [43]. Adding additional sensors could help avoid false positives.

However, if the sensors are from different manufacturers, then current smart home systems cannot support this feature, even though trigger-action programming is a start. Using concurrent sensor readings to reduce errors in the system is one example of using collective information from different devices. More research is required to explore the possibilities of the collective information we could get from a connected network of devices.

C. Customized Learning and Scheduling

Our results echoed the findings from prior work [8] that smart thermostats' learning capabilities fall short, particularly in multi-user environments or for users with variable schedules. It is necessary to give users greater transparency about what exactly the learning thermostat has guessed about the household's schedule, as well as a richer channel for users to indicate what the thermostat should either remember or ignore. Furthermore, context matters. If someone visits the house, they may change the temperature, but their preferences should be forgotten once they leave. This could be detected by other sensors, such as a decrease of motion in the guest room, or even the decreased number of connected smartphones. Devices' built-in learning features should also detect conflicts in preference among family members, guiding users toward a fair resolution. Therefore, while introducing learning processes to a smart home causes some trouble, by collaborating with other sensors, it is possible for these smart devices to better understand contexts, increase robustness towards uncertainties in daily life, and thus make more sensible decisions for users.

D. Smart Home Simulation

Participants, particularly non-technical ones, commonly worried that automation rules they created would malfunction

or otherwise break the system. Without proper testing, non-technical users might have a hard time predicting the behaviors of their smart home system, which not only makes them lose control of their own home and discourages them from trying, but also creates uncertainty regarding the real cause of some abnormal activities, which could benefit an attacker or intruder.

Prior work has proposed retroactive visualizations of what has happened in a smart home [9], [23]. We instead propose a home simulator that enables users to test the potential effect of rules before activating them. Such simulations could allow users to test rules under rare or special conditions, such as infrequent weather events, thus increasing user confidence in the rules they write. With the help of formal analysis and modeling [32], a simulator could even help users identify corner cases and unforeseen consequences.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grants No. 1756011 and 1837120.

REFERENCES

[1] Statista, "Smart home report 2018," https://www.statista.com/outlook/279/109/smart-home/united-states, 2018.
[2] S. Mennicken, J. Vermeulen, and E. M. Huang, "From today's augmented houses to tomorrow's smart homes: New directions for home automation research," in Proc. UbiComp, 2014.
[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 Proc. CHI, 2017.
[4] A. M. Davani, A. A. N. Shirehjini, and S. Daraei, "Towards interacting with smarter systems," Journal of Ambient Intelligence and Humanized Computing, vol. 9, no. 1, pp. 187–209, 2018.
[5] S. Mare, L. Girvin, F. Roesner, and T. Kohno, "Consumer smart homes: Where we are and where we need to go," in Proc. HotMobile, 2019.
[6] K. Gram-Hanssen and S. J. Darby, ""Home is where the smart is"? evaluating smart home research and approaches against the concept of home," Energy Research & Social Science, vol. 37, pp. 94–101, 2018.
[7] J.-b. Woo and Y.-k. Lim, "User experience in do-it-yourself-style smart homes," in Proc. UbiComp, 2015.
[8] R. Yang and M. W. Newman, "Learning from a learning thermostat: Lessons for intelligent systems for the home," in Proc. UbiComp, 2013.
[9] S. Mennicken, D. Kim, and E. M. Huang, "Integrating the smart home into the digital calendar," in Proc. CHI, 2016.
[10] A. A. Nacci, B. Balaji, P. Spoletini, R. Gupta, D. Sciuto, and Y. Agarwal, "Buildingrules: A trigger-action based system to manage complex commercial buildings," in Proc. UbiComp Adjunct, 2015.
[11] E. Zeng, S. Mare, and F. Roesner, "End user security & privacy concerns with smart homes," in Proc. SOUPS, 2017.
[12] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur, "Rethinking authentication and access control for the home Internet of Things (IoT)," in Proc. USENIX Security Symposium, 2018.
[13] B. Ur, J. Jung, and S. Schechter, "Intruders versus intrusiveness: Teens' and parents' perspectives on home-entryway surveillance," in Proc. UbiComp, 2014.
[14] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell, ""A stalker's paradise": How intimate partner abusers exploit technology," in Proc. CHI, 2018.
[15] D. Kumar, R. Paccagnella, P. Murley, E. Hennenfent, J. Mason, A. Bates, and M. Bailey, "Skill squatting attacks on Amazon Alexa," in Proc. USENIX Security, 2018.
[16] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, and F. Qian, "Understanding and mitigating the security risks of voice-controlled third-party skills on Amazon Alexa and Google Home," 2019.
[17] G. Ghiani, M. Manca, F. Paternò, and C. Santoro, "Personalization of context-dependent applications through trigger-action rules," ACM TOCHI, vol. 24, no. 2, p. 14, 2017.
[18] B. Ur, E. McManus, M. Pak Yong Ho, and M. L. Littman, "Practical trigger-action programming in the smart home," in Proc. CHI, 2014.
[19] J. Brich, M. Walch, M. Rietzler, M. Weber, and F. Schaub, "Exploring end user programming needs in home automation," ACM TOCHI, vol. 24, no. 2, p. 11, 2017.
[20] J. Huang and M. Cakmak, "Supporting mental model accuracy in trigger-action programming," in Proc. UbiComp, 2015.
[21] L. Yarosh and P. Zave, "Locked or not?: Mental models of IoT feature interaction," in Proc. CHI, 2017.
[22] W. Brackenbury, A. Deora, J. Ritchey, J. Vallee, W. He, G. Wang, M. L. Littman, and B. Ur, "How users interpret bugs in trigger-action programming," in Proc. CHI, 2019.
[23] N. Castelli, C. Ogonowski, T. Jakobi, M. Stein, G. Stevens, and V. Wulf, "What happened in my home?: An end-user development approach for smart home data visualization," in Proc. CHI, 2017.
[24] T.-H. K. Huang, A. Azaria, and J. P. Bigham, "Instructablecrowd: Creating if-then rules via conversations with the crowd," in Proc. CHI Extended Abstracts, 2016.
[25] X. Chen, C. Liu, R. Shin, D. Song, and M. Chen, "Latent attention for if-then program synthesis," in Proc. NIPS, 2016.
[26] C. Quirk, R. Mooney, and M. Galley, "Language to code: Learning semantic parsers for if-this-then-that recipes," in Proc. ACL, 2015.
[27] J. Fiorenza and A. Mariani, "Improving trigger action programming in smart buildings through suggestions based on behavioral graphs analysis," Politecnico di Milano, Tech. Rep., 2015.
[28] C. Nandi and M. D. Ernst, "Automatic trigger generation for rule-based smart homes," in Proc. PLAS, 2016.
[29] Z. B. Celik, P. McDaniel, and G. Tan, "SOTERIA: Automated IoT safety and security analysis," in Proc. USENIX ATC, 2018.
[30] C.-J. M. Liang, L. Bu, Z. Li, J. Zhang, S. Han, B. F. Karlsson, D. Zhang, and F. Zhao, "Systematically debugging IoT control system correctness for building automation," in Proc. BuildSys, 2016.
[31] L. Bu, W. Xiong, C.-J. M. Liang, S. Han, D. Zhang, S. Lin, and X. Li, "Systematically ensuring the confidence of real-time home automation IoT systems," ACM TCPS, vol. 2, no. 3, p. 22, 2018.
[32] L. Zhang, W. He, J. Martinez, N. Brackenbury, S. Lu, and B. Ur, "Synthesizing and repairing trigger-action programs using LTL properties," in Proc. ICSE, 2019.
[33] Q. Wang, W. U. Hassan, A. Bates, and C. Gunter, "Fear and logging in the Internet of Things," in Proc. NDSS, 2018.
[34] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash, "Flowfence: Practical data protection for emerging IoT application frameworks," in Proc. USENIX Security Symposium, 2016.
[35] Z. B. Celik, L. Babun, A. K. Sikder, H. Aksu, G. Tan, P. McDaniel, and A. S. Uluagac, "Sensitive information tracking in commodity IoT," in Proc. USENIX Security, 2018.
[36] I. Bastys, M. Balliu, and A. Sabelfeld, "If this then what?: Controlling flows in IoT apps," in Proc. CCS, 2018.
[37] M. Surbatovich, J. Aljuraidan, L. Bauer, A. Das, and L. Jia, "Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of IFTTT recipes," in Proc. WWW, 2017.
[38] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Decentralized action integrity for trigger-action IoT platforms," 2018.
[39] A. Rahmati, E. Fernandes, K. Eykholt, and A. Prakash, "Tyche: A risk-based permission model for smart homes," in Proc. SecDev, 2018.
[40] A. Strauss and J. Corbin, Basics of qualitative research. Sage publications, 1990.
[41] IFTTT, https://ifttt.com, 2018.
[42] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," IEEE TCNS, vol. 4, no. 1, pp. 49–59, March 2017.
[43] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," in Proc. ACC, 2015.

APPENDIX

The relevant sections of our survey instrument follow:

Please read this definition carefully because we will use it throughout the survey. The devices discussed in this survey are home devices and appliances that can connect to the Internet and each other. Internet-connected lights, thermostats, cooking devices, locks, outdoor equipment, cameras, and similar devices are all included in this definition.

However, voice assistants (e.g., Alexa), computers, smartphones, tablets are not considered to be internet-connected home devices in this study.

What kind of internet-connected houshold devices have you used? Check all that apply.
◯ Internet-connected camera ◯ Internet-connected cooking device ◯ Internet-connected door lock ◯ Internet-connected light ◯ Internet-connected outdoor device (sprinkler, mower, etc.) ◯ Internet-connected thermostat ◯ Device(s) not listed here

[Optional] If you remember, please specify the brand name of the smart home device you have. If you have multiple devices, please separate them with commas.
Internet-connected camera:
Internet-connected cooking device:
Internet-connected door lock:
Internet-connected light:
Internet-connected outdoor device (sprinkler, mower, etc.):
Internet-connected thermostat:
Device(s) not listed here:

Many internet-connected houshold devices are vulnerable to network failures or power failures.
Have you ever had any frustrating experiences with network failures or power failures with your internet-connected household devices?
◯ Yes ◯ No

[If "Yes"] Please tell us about the frustrations you have encountered.

[If "No"] Have you heard about anyone you know having any frustrating experiences with network failures or power failures with their internet-connected houshold devices?
◯ Yes ◯ No

[If "Yes"] Please tell us about the frustrations they have encountered.

[If "No"] Can you imagine any difficulties you might expect to have regarding power failures or network connectivity issues for internet-connected household devices? Please tell us about them.

Most internet-connected household devices have some built-in features.
Some examples: 1) An internet-connected thermostat can learn your preferences and set the temperature for you automatically. 2) A smart vacuum robot can detect obstacles, even if you don't give it any information about the layout of your room. 3) Your smart camera may enable motion-detection by default.
Have you ever had any frustrating experiences with these built-in features with your internet-connected household devices?
◯ Yes ◯ No

[If "Yes"] Please tell us about the frustrations you have encountered.

[If "No"] Have you heard about anyone you know having any frustrating experiences with built-in features of their internet-connected houshold devices?
◯ Yes ◯ No

[If "Yes"] Please tell us about the frustrations they have encountered.

[If "No"] Can you imagine any difficulties you might expect to have with built-in features of internet-connected household devices? Please tell us about them.

Many smart home platforms let you set up if-then rules (e.g., IFTTT or Samsung SmartRules) or write computer programs/code (e.g., Java, Python, C++) to control your devices. For example, you could set up an if-then rule or write a program/code to make your smart lights turn on automatically whenever someone opens the door.
Have you ever done so?
◯ I have both written rules and programs/code to control my devices. ◯ I have written rules to control my devices, but I have never written programs/code to do so. ◯ I have written programs/code to do control my devices, but I have never written rules to do so. ◯ I have never done either.

[If "I have never done either" is not chosen] Have you ever had any frustrating experiences writing rules or programs/code to control your internet-connected household devices?
◯ Yes ◯ No

[If "Yes"] Please tell us about the frustrations you have encountered.

[If "No"] Have you heard about anyone you know having any frustrating experiences writing rules or programs/code to control your internet-connected household devices?
◯ Yes ◯ No

[If "Yes"] Please tell us about the frustrations they have encountered.

[If "No" or "I have never done either"] Can you imagine any difficulties you might expect to have writing rules or programs/code to control internet-connected household devices? Please tell us about them.

Have you experienced any other frustrating experiences with internet-connected household devices that we did not mention above?
◯ Yes ◯ No

[If "Yes"] Please tell us about the frustrations you have encountered.

[If "No"] Have you heard about anyone you know having any other frustrating experiences with internet-connected household devices that we did not mention above?
◯ Yes ◯ No

[If "Yes"] Please tell us about the frustrations they have encountered.

[If "No"] Can you imagine any difficulties not yet mentioned you might expect to have with internet-connected household devices? Please tell us about them.