Smart Home Updates: User Perceptions and Experiences

Julie M. Haney
National Institute of Standards and Technology

Susanne M. Furman
National Institute of Standards and Technology

Abstract

Smart home device updates are important tools for users to remediate security vulnerabilities and protect devices from future attacks. However, no prior research has been conducted to understand smart home users' perceptions of and experiences with updates. To begin to address this gap, we analyzed update-related data from a broader in-depth interview study of 40 smart home users. Preliminary results indicate that users experienced inconsistency in update transparency and methods, as well as confusion about how and if updates were applied. In addition, most users did not relate smart home device updates to security, so they might not have been as inclined to install updates in a timely fashion. Since updates were not a primary focus of the interview study, we are planning a follow-up survey to a broader population to more deeply examine update perceptions and experiences on a per-device basis. Our efforts will provide a new understanding of smart home updates from a usable security perspective. We hope to identify similarities to prior research focused on updates for other types of computing devices while discovering ways in which smart home device updates may be different or more challenging. Our results may also inform the design of a more usable platform for smart home updates.

1 Introduction

Smart home updates are a critical mechanism by which manufacturers can distribute patches to remediate security vulnerabilities. Updates may be one of the few tools users have to secure their devices since other configurable security options are limited or unavailable. Unfortunately, update mechanisms are often inconsistent across devices [5]. Even among security professionals, the number one threat to IoT was viewed as "difficulty patching Things, leaving them vulnerable" [12]. How then can manufacturers design update mechanisms that are consistent and easy for end users to understand and implement?

To better understand users' experiences and challenges with smart home updates, we analyzed update-related data from a broader, in-depth interview study of 40 smart home users aimed at investigating their general experiences with, perceptions of, and opinions about smart home devices, including aspects of privacy and security. By exploring this subset of the interview data, we begin to gain insights into perceptions of and challenges with updates, including what role, if any, users perceive updates as playing with the security of their devices.

Our preliminary observations show that users experience inconsistency in update transparency and methods, as well as confusion about how and if updates are applied. More concerning, most study participants did not relate smart home device updates to security, so they might not have been as inclined to install updates in a timely fashion.

Since updates were not a major focus of the interview study, we wish to delve deeper into user update experiences and perceptions, especially on a per-device basis. To that end, we are planning a follow-up survey to gather responses from a broader population of smart home owners.

When completed, we hope our research will have several contributions. To the best of our knowledge, we are the first user-centered effort to explore end user experiences and challenges with updates within the context of smart home devices from both a usability and security perspective. We hope to identify similarities to prior research focused on updates of other types of computing devices while discovering ways in which smart home device updates may be different or more challenging. Our results may also inform the design of smart home device update mechanisms and notifications to provide a more usable platform for deploying critical security patches

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Boston, MA, USA.

when necessary.

2 Related Work

While no prior studies have explored user update behaviors for smart home technologies, researchers have investigated these behaviors for traditional IT. Investigators discovered that people delayed software updates for a number of reasons, including: a lack of awareness of or information pertaining to the value of the upgrade; interruption of computing activities; and possible negative consequences of applying the update [4, 11, 13]. Fagan et al. [4] suggested that people have a difficult time understanding the relationship between software updates and security. Vaniea and Rashidi [14] found that, ultimately, users must balance the risk and costs of updating against the potential benefits. The researchers recommended that manufacturers make it easy for users to find information about updates and that a recovery path be provided should updates cause unintended consequences.

A number of critical security vulnerabilities for smart home devices have been identified in recent years [1], highlighting the need for timely updates [2, 9]. However, there are unique challenges to IoT updates [6]. Among those challenges, IoT manufacturers may be inexperienced with designing security features and update mechanisms. Economic incentives for providing updates and long-term support for these inexpensive and disposable devices may not exist, leaving devices vulnerable to attack.

Emami-Naeini et al. [3] interviewed smart home users, noting that most desired automatic updates because of convenience. Lin and Bergmann [10] suggested that smart home devices should implement updates with little or no user intervention. Researchers at the U.S. National Institute of Standards and Technology (NIST) discovered that information on updates is not always readily available to consumers and that updates are not always done in a secure manner [5]. Therefore, they recommended that IoT manufacturers notify users about updates in a timely fashion and allow for rollback should an error occur. However, to the best of our knowledge, no prior literature addresses user perceptions of and experiences with smart home updates in detail.

3 Methodology

From February to June 2019, we interviewed 40 smart home users to understand their perceptions of and experiences with smart home devices. Our institution's research protections office approved the study. Prior to the interviews, we informed participants of the study purpose and how their data would be protected. Data were recorded with generic identifiers (e.g., P14_U) and not linked back to individuals.

We hired a consumer research company to recruit adult users of smart home devices from a database of individuals living in a large U.S. metropolitan area who had agreed to be contacted about research opportunities. To determine eligibility, prospective participants completed an online screening survey about their smart home devices, their role with the devices (e.g., administrator, user), and other demographic information. After reviewing the screening information, we selected participants if they were active users of at least two different types of smart home devices. In line with current interview compensation rates in our region, participants were given a $75 prepaid card.

Participants had diverse professional backgrounds with only eight in an engineering or IT field. Thirty-two of the 40 participants had installed and administered their devices (indicated with an A after the participant ID), and eight were non-administrative users of the devices (indicated with a U). 55% were male and 45% were female. Seventy percent were between the ages of 30 and 49. Participants were highly educated with 45% having a master's degree or above and another 50% with a BS/BA. All but one participant had three or more individual smart home devices, with 38 having three or more different categories of devices.

We collected data via 40 semi-structured interviews lasting on average 41 minutes. Interview questions covered several topics: purchase and general use; installation and maintenance (including updates); privacy; security; and safety. In this paper, we focus only on collected data pertaining to updates. All interviews were audio recorded and transcribed.

We analyzed the interview data using both deductive and inductive coding practices. Initially, each member of the research team individually coded a subset of four interview transcripts using an *a priori* code list based on research questions and open coded for additional concepts as needed. We then met to discuss codes and develop a codebook. Coding then continued until all transcripts were coded by two researchers, who then met to examine and resolve differences in code application and identify relationships between the codes and central themes.

4 Preliminary Results

4.1 Update Purpose and Urgency

Participants most often viewed updates as fixing or adding non-security functionality. Interestingly, this perception led to mixed feelings regarding the urgency of applying updates. Several participants who had experienced issues with their devices believed updates were a high priority. A participant who owns a smart video doorbell and security cameras noted that smart home devices *"would have the highest priorities than any of the other apps on my phone... because that's the security of my home"* (P31_A).

However, others thought functionality updates were lower priority or unnecessary as long as the device appeared to be working properly. For example, a participant described her

indifference with respect to updates, *"I don't think that the end user actually really cares. As long as the thing works, it works"* (P40_U). Other participants did not feel they could properly assess the criticality of the update because the manufacturer did not reveal the purpose of the update.

4.2 Update Modes and Notifications

The interviews revealed that update modes may vary from smart home device to device, with some updating automatically and others requiring users to manually initiate updates. In addition, participants discovered available updates in different ways depending on the device. A participant who owned multiple devices said: *"Some of them notify me, others update automatically, and others I'll find out about either through an email or just because I'm kind of monitoring technology news in general"* (P15_A).

Smart home devices that notify users of available updates do so in a variety of ways. Notifications "pushed" to the device's user interface or via the companion app before or after update installation are most common. For example, an owner of a smart doorbell explained how she finds out about updates: *"I see an alert. It says, 'Your Ring doorbell has a new update. Do you want to allow it? Do you want to accept it?' "* (P36_A). Several participants received emails alerting them of available or just-installed updates. Some devices with screen interfaces, such as smart thermostats and televisions, displayed the update notification directly on the device itself. Other smart home owners did not receive push notifications to tell them updates were available. Rather, they had to manually open the companion app and check.

4.3 Uncertainty about Update Status

Inconsistencies in update mechanisms may result in confusion about update status. Users may not observe update notifications, do not recall setting an option to automatically install updates, or are not sure if there are configurable options for setting update parameters. This may lead to a sense of uncertainty about whether their devices are being updated or even can be updated. One user remarked about his virtual assistant, *"I don't know when it's [virtual assistant] doing its updates. Like ever. They never ask me. They never prompt me"* (P7_A).

Some participants assumed that the lack of notifications meant that updates must be happening automatically. While possibly true with some devices, this assumption might be flawed for other products. A participant lamented, *"They don't notify me when there's an update. I guess I just kind of assume that they happen as they go. You would think that I'd get an email, but I guess I don't. That might be nice" (P23_A).*

Even though some users may have an assumption of automatic updates, the uncertainty due to lack of notification leaves them with a sense of discomfort. For example, one participant stated: *"I'm assuming that updates are being done silently in the background... It sort of gives the impression that you bought this thing and it's not evolving... that it's not expanding and getting new updates"* (P24_A).

4.4 Updates to Apps vs. Updates to Devices

In addition to general uncertainty about update status, the interviews revealed that participants often conflated updates to smart home device companion app software (typically installed on a smartphone) with updates to device firmware. They did not realize that updates to apps were not necessarily accompanied by device updates and vice-versa. This was evidenced by participants referencing typical smartphone app update indicators when asked how they know smart home device updates are available. For example, a user of an Android-based phone explained:

> *"I get a notification. It doesn't say specifically which apps need to be updated. It just says 48 apps need to be updated. Then I go into Google Play, and see my apps, and individually determine which ones I want to update"* (P31_A).

4.5 Update Concerns

Even when update availability was visible, participants voiced concerns about updates causing issues or breaking functionality on their smart home devices. For example, one participant voiced frustration with updates to his smart television: *"I've had to reset my TVs many times because the software update didn't work or kind of messed things up"* (P10_A). Updates also have the potential to invalidate previous user configuration settings or necessitate new ones: *"as they come out with updates, particularly significant updates that change the interface, for example, that might be cause for me to go back in and redo some of the settings"* (P15_A).

Two participants expressed concerns about a lack of updates should a manufacturer stop supporting a product. One of these commented:

> *"I would hope that over time the companies that support these devices would continue to update their firmware and basically make them more reliable. I think in some cases that's happened, but I think in other cases the devices just get abandoned"* (P11_A).

4.6 Relationship to Security

Although update mechanisms are a conduit to fix security vulnerabilities in smart home devices, study participants rarely linked updates to security, with only five mentioning updates in the context of security. When asked what mitigation actions they take to address any security concerns they might have, only three mentioned applying updates or upgrading

products: *"I'm updating everything a lot more...keeping up with the technology because it is so important" (P31_A).*

Interestingly, two participants recognized the importance of applying updates, but were concerned about potential security-related consequences. One participant liked that updates to his devices could be done via the internet, but at the same time was concerned because *"it means that someone's reaching in... There's some kind of access from the outside"* (P26_A). Another saw potential for updates to weaken security:

> *"I guess one area where I would be worried about would be adding features that may threaten my privacy and security... I would want to know that the update also gave me the capability of disabling or turning off that feature"* (P15_A).

5 Discussion

5.1 Comparison to Traditional Updates

We note similarities between our results and those from previous research studies related to updates for traditional IT. Similarities included: a lack of awareness of the importance of applying updates [4, 11, 13]; a lack of information about the update purpose hindering users' ability to weigh risk and cost against potential update benefits [11, 14]; concern about possible negative consequences of applying updates [4, 11, 13]; and concern about surprise new features being added [13].

Although similarities exist, we identified several differences in user experiences with smart home updates as compared to updates explored in prior studies. We did not find evidence of concerns about interruption (e.g., as noted in [11]), likely because users do not have the same kind of interactive sessions with smart devices as they would on a tablet, phone, or computer. Our findings additionally suggest that, because devices are often controlled with a mobile companion app, some updates may be overlooked since several participants did not understand the difference between a phone update, an app update, and a device update. We also discovered that participants were concerned about manufacturers discontinuing product support (and therefore, no longer issuing updates) due to the dynamic smart home market. As opposed to updates for more-familiar and widely-used operating systems, applications, and hardware (e.g., those from Apple and Microsoft), our participants were often unaware if updates were available, how to configure automatic updates, or how to check update status. Confusion about update mechanisms may be amplified by the number of smart home devices users own, especially if the products are from various manufacturers with different update models and different modes of notification.

5.2 Informing Usable Updates

Study results may inform more usable update interfaces and mechanisms. Insufficient information about the purpose and benefit of updates may result in users lacking a sense of urgency about applying updates, especially if devices appear to be working fine. Users may also be uncertain about update status and availability. To help users make informed decisions, manufacturers could provide greater transparency of update purpose and importance of applying an update (perhaps via a criticality rating), which is in concert with Vaniea and Rashidi's recommendation for easy-to-find information on updates [14]. As also recommended by the FTC [6], manufacturers could be more forthcoming about their update model and support so that users are aware of how update availability will be made known, what actions users should take to install updates, what update configuration and notification options (if any) are available, and how manufacturers will handle discontinuation of product support.

In addition to lack of transparency, many of our participants expressed discomfort or frustration with updates and their ability to control them. Providing additional information on updates can help users feel more confident in their update decisions. In addition, manufacturers could provide options for users to configure automated updates (as recommended in [10]) with configurable notifications of success afterwards. Users could be given options to schedule if and when they receive notifications. To mitigate concerns that updates might break the device or result in unwanted features or settings, devices could support a rollback mechanism, as recommended by others [5, 8, 14]. Users may then be more likely to install an update if they have a way out should there be a problem.

6 Limitations and Planned Future Work

In addition to typical limitations of interview studies (e.g., self-report and social desirability biases), our study results may have limited generalizability. Our sampling frame of mostly well-educated individuals living in a high-income region may not be fully representative of the U.S. smart home user population. However, our participant population does appear to typify early adopters of smart home devices as identified in industry surveys (for example, [7]).

Our interview study was meant to be exploratory with a goal of identifying areas warranting additional investigation. As such, the interview protocol was broad in covering multiple aspects of smart home ownership and did not focus solely on updates. We also did not ask about updates on a per-device basis (instead, asking about general update experiences), so are not able to determine if differences exist depending on the type of device and manufacturer. In recognition that more research should be done to delve deeper into users' smart home update experiences, we are in the initial planning phase for an online, quantitative survey of a larger, more diverse sample of U.S. smart home users. In addition to asking more questions about perceptions of updates (e.g., importance, purpose), we will obtain per-device experiences and explore what kind of update options, if any, users would like.

Disclaimer

Certain commercial companies or products are identified in this paper to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

References

[1] Bitdefender. The IoT threat landscape and top smart home vulnerabilities in 2018. https://www.bitdefender.com/files/News/CaseStudies/study/229/Bitdefender-Whitepaper-The-IoT-Threat-Landscape-and-Top-Smart-Home-Vulnerabilities-in-2018.pdf, 2019.

[2] Consumer Product Safety Commission. Status report on the Internet of Things (IoT) and consumer product safety. https://www.cpsc.gov/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf?6sv9HwTXKHrkdmAyAkQ0_TsKCkpl1lR2, 2019.

[3] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 2019.

[4] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior*, 51:504–519, 2015.

[5] Michael Fagan, Mary Yang, Allen Tan, Lora Randolph, and Karen Scarfone. Draft NISTIR 8267 Security review of consumer home Internet of Things (IoT) products. Technical report, National Institute of Standards and Technology, 2019.

[6] Federal Trade Commission. Internet of things privacy and security in a connected world. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, 2015.

[7] GfK. Future of smart home study global report. https://www.gfk.com, 2016.

[8] IoT Security Foundation. Secure design best practice guides. https://www.iotsecurityfoundation.org/wp-content/uploads/2019/11/Best-Practice-Guides-Release-2.pdf, 2019.

[9] Ari Lazurus. Update your software now. https://www.consumer.ftc.gov/blog/2019/06/update-your-software-now, 2019. Federal Trade Commission.

[10] Huichen Lin and Neil Bergmann. IoT privacy and security challenges for smart home environments. *Information*, 7(3):44, 2016.

[11] Arunesh Mathur, Josefine Engel, Sonam Sobti, Victoria Chang, and Marshini Chetty. "They Keep Coming Back Like Zombies": Improving software updating interfaces. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 16)*, pages 43–58, 2016.

[12] SANS Institute. Securing the Internet of Things survey. https://www.sans.org/reading-room/whitepapers/covert/paper/34785, 2014.

[13] Kami Vaniea, Emilee Rader, and Rick Wash. Betrayed by updates: How negative experiences affect future security. In *Proceedings of the 2014 SIGCHI Conference on Human Factors in Computing Systems (CHI 14)*, pages 2671–2674, 2014.

[14] Kami Vaniea and Yasmeen Rashidi. Tales of software updates: The process of updating software. In *Proceedings of the 2016 SIGCHI Conference on Human Factors in Computing Systems (CHI 16)*, pages 3215–3226, 2016.