Transferring Update Behavior from Smartphones to Smart Consumer Devices

Matthias Fassl[1,2(✉)], Michaela Neumayr[1], Oliver Schedler[1], and Katharina Krombholz[1]

[1] CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
{matthias.fassl,neumayr,oliver.schedler,krombholz}@cispa.de
[2] Saarland University, Saarbrücken, Germany

Abstract. Automatic updates are becoming increasingly common, which minimizes the amount of update decisions that users have to make. Rapidly deployed important updates have a major impact on security. However, automatic updates also reduce the users' opportunities to build useful mental models which makes decision-making harder on other consumer devices without automatic updates. Users generally transfer their understanding from domains that they know well (i.e. smartphones) to others. We investigate how well this transfer process works with respect to updates and if users with automatic updates fare worse than those with manual updates.

We conducted a formative field study ($N = 52$) to observe users' update settings on smartphones and examine reasons for their (de-) activation. Based on the results, we conducted an online survey ($N = 91$) to compare how users perceive update notifications for smartphones and smart consumer devices. One of our main findings is that update decisions based on *expected changes* do not apply well to these devices since participants do not expect meaningful and visual changes. We suggest naming updates for such devices 'maintenance' to move users' expectations from 'new features' to 'ensuring future functionality'.

1 Introduction

Keeping systems and software up to date is the most common expert advice for securing devices [11,20]. Consequently, prior work extensively studied update attitudes and behavior [12,13,23,24,26,27]. Vendors introduced partially or fully automatic updates since users often delay or skip updates. Windows 10 introduced intervention-less automatic update downloads and installation, Android and iOS introduced automatic updates, and Google Chrome started using silent automatic updates over ten years ago. Automatic updates improve the rate and speed of update deployment [3]. However, automatic updates create two potential pitfalls: (1) Users feel betrayed as soon as automated systems make choices that defy their expectations [4] and these incidents will impact all future update decisions [26]; (2) Automated updates reduce users' understanding of what is happening on their computers [27]. These pitfalls diminish users' ability to make informed decisions when updates cannot be fully automated.

S. Katsikas et al. (Eds.): ESORICS 2021 Workshops, LNCS 13106, pp. 357–383, 2022.
https://doi.org/10.1007/978-3-030-95484-0_21

Update behaviors and attitudes on desktops and smartphones are well studied [3–5,7,12–15,23–27]. However, smart consumer devices with minimalistic user interfaces (UIs) and inconspicuous computing power became common after the Internet-of-Things emerged. Gartner predicted 20.8 billion IoT devices for 2020, thereof 13.5 billion consumer devices [16]. In contrast to communication and entertainment heavy smartphones, IoT devices control day-to-day life. Some smart consumer devices, e.g., dishwashers, have very minimal UIs, impacting how users perceive and handle updates. However, there is still little research on how users transfer update behavior to other application areas beyond smartphones and desktops. Automatic updates alleviate some update issues. However, sometimes they are neither practical nor safe, and maybe not even possible for devices with limited UIs – making questions on user understanding and engagement even more pressing [1,21]. Since traditional computing devices move towards automatic updates, awareness of updates' effects and importance decreases. However, users may have to decide on updates again when handling smart consumer devices. It remains unclear how users make their update decisions on these devices and how they transfer their update-knowledge from traditional computing devices.

The aim of this work is (1) to study users' reasons for (de-)activating automatic updates, (2) to understand how users handle manual update decisions on smartphones, and (3) to evaluate if their update reasoning is transferable to smart consumer devices found in the IoT. We conducted an exploratory field study ($N = 52$) on users' reasons for deactivating automatic updates. We used a mixed-methods online survey ($N = 91$) to explore how automatic updates affect users' manual update decisions and how users transfer their update behavior smart consumer devices (in our study: dishwasher, self-lacing shoes, and a modern car). Our main contributions are: (1) we **observed an increased rate of automatic updates** for smartphone apps (compared to Tian et al. [23]) and provide **ranked lists of reasons for (de)activating automatic updates**; (2) we **describe the differences between users that activated automatic updates and those who did not** (3) we discuss how **transferring users' update behavior to smart consumer devices might fail** since two main strategies (evaluation by expected changes and evaluation by notification) are difficult to apply to smart consumer devices; (4) we provide **design implications** for smart consumer device updates.

2 Methodology

Guided by the following research questions, we study how automatic updates affect users' remaining update decisions on smartphones and how well these decisions transfer to smart consumer devices.

RQ1: How common is deactivation of automatic updates and what are the users' reasons for it?

RQ2: How do users' update attitudes (information demand, perceived importance, and expected effects) transfer from smartphones to smart consumer devices?

Our *formative field study* establishes the share of users who (do not) use automatic updates and their (de)activation reasons. Based on these results, we designed an *online survey* which compares how participants make update decisions on smartphones and smart consumer devices. We explained the purpose, the procedure, and the type of questions to all study participants. We did not collect identifying information and instructed participants to provide screenshots without identifiers.

All participants gave us their informed consent. We compensated participants for their time, based on the minimum wage. Our university's ethical review board approved this study.

2.1 Formative Field Study

In the formative field study ($N = 52$), we collected the participants' OS version, the OS update settings (if applicable), and update settings for installed apps. We asked open-ended questions to understand their reasons for changing settings. Afterwards we used a questionnaire to collect demographic data. Section B presents the entire questionnaire. We conducted a pre-study with 8 participants. For three days, we recruited participants with Android or Apple phones in front of our university's dining hall during lunch time. Table 3 in the Appendix presents the demographics.

We analyzed the observed frequencies of smartphone OS settings. We used *open coding* to evaluate qualitative free-response data. Two researchers independently coded the responses and constructed two independent codebooks, then constructed a common codebook (see Sect. C) and resolved all disagreements.

2.2 Online Survey

The formative field study showed that participants like to maintain control over installed software. They preferred to update apps they considered important and influence the installation time to avoid bugs and data-loss, confirming previous work [5,15,25,26].

Questionnaire. We used those results to construct an online survey on Amazon MTurk ($N = 91$) which exposed participants to five different update scenarios, two for mobile phones (system and app update) and three concerning smart consumer devices (dishwasher, shoes, car). Appendix E shows the notifications that we used in the survey. We chose update scenarios that (1) concern devices with a low barrier to use – so most participants could imagine a use-case for them, and (2) includes an update decision that participants will not have faced before. Similarily, Fagan et al. [5] used fictional update notifications to understand users' update behaviors and attitudes. For each update notification, we asked participants to explain the update's importance, what kind of changes they expect, when they would prefer to install it, and how they would redesign the notification.

To evaluate users' responses in context we also asked for their update settings (phone OS version, screenshots of OS and app update settings), their potential update avoidance behavior (connected to WiFi and charging habits), and their 5-point Likert evaluation of (de)activation reasons. Since prior work [9] suggests that update behavior depends on technology-savyness, sense of autonomy, and personality, we added appropriate psychometric scales (Affinity for Technology Interaction (ATI) [8], Reactance to Autonomy [10], and Big Five Inventory (BFI-K) [18]). We asked for general demographic information such as gender, occupation, educational background, and household income and added three attention check questions throughout the survey. Section D in the Appendix presents the full questionnaire (translated into English).

Evaluation. We used a repeated-measures ANOVA to find significant differences between perceived importance of the five notifications. We evaluated the open-ended responses to the five notifications with thematic analysis [2]. Two researchers used *open coding* to independently assign initial codes to their part of the data. They used the other's initial codebook to independently code the remaining data, resulting in an inter-coder reliability (ICA) of Brennan and Prediger's $\kappa = 0.63$. In an iterative approach, the two researchers discussed the categories with the most mismatches, renamed or merged codes, and revised the segments in questions, resulting in an inter-coder reliability (ICA) of Brennan and Prediger's $\kappa = 0.83$. During the last session they used *axial coding* to restructured the entire codebook and identify themes. Section F in the Appendix contains the final codebook (containing 8 categories with a total of 70 codes).

To understand how well update decisions transfer to smart consumer devices, we qualitatively compare users responses according to their update preferences (automatic vs. manual) and the type of notification they responded to (smartphone vs. smart consumer device). We report differences between those groups if: (1) codes are not included in both groups, (2) the most frequently assigned codes are different, or (3) if a code was assigned three times more often in one group.

Recruitment and Participants. After conducting a pilot study ($N = 3$), we recruited Amazon MTurk workers from Germany with an approval rate of 99.0% and compensated them with USD 5.60. We excluded five of 96 participants, either because the GeoIP results showed that they were not in Germany or two researchers independently agreed that their provided answers did not answer the open questions. Table 6 in the Appendix presents the demographics.

3 Results

We report the prevalence of automatic updates that we observed in our formative field study and our online survey in Sect. 3.1. Using that information we evaluate (in Subsect. 3.2) how activated automatic updates influence the participants' responses to the shown update notifications. In Subsect. 3.3 we describe how

participants decide if and when they would like to install updates and how well this decision-process transfers from smartphones to smart consumer devices. During the evaluation we found several contradicting user requirements which we present in Subsect. 3.4.

3.1 Automatic Update Settings and Reasons for (De)activation

Most of the participants in the formative field study did not change default update settings. Almost all Android users had operating system updates enabled and used the "WiFi only" option for application updates (the default). Most iOS users had activated OS updates, but more than a third of them deactivated automatic application updates. Table 4 in the Appendix shows a summary of the observed update settings. Table 5 compares update settings of users with high ($\geq$4) and low ($<$4) self-efficacy scores. Participants most commonly mentioned three types of security-relevant practices that they did on a regular basis: *authentication*, *privacy settings*, and *abstention* from potentially useful products or features. Even though our study procedure primed all participants on updates, only four participants mentioned that they regularly apply updates to keep their mobile secure. In the online survey 63 (69%) participants had an Android phone, whereas 28 (31%) had an iPhone. By default, Android enables automatic OS updates, and iOS will ask during the initial setup. 52 participants (57%) had automatic OS updates enabled, 17 (19%) had them disabled, and 22 (24%) did not submit a suitable screenshot. By default, both Android and iOS enable automatic app updates. 79 participants (87%) had enabled automatic app updates, 10 (11%) disabled them, and 2 (2%) did not submit a suitable screenshot.

In the formative field study, the two most common reasons for deactivating updates were the wish to maintain control over installed software or concerns about data usage. Two aspects of maintaining control came up: (1) participants only wanted increased agency over updates for apps they perceived as important enough, and (2) they would like to decide when to install an update since they know from experience that new updates may have bugs and could lead to data-loss. In the formative field study the two most common reasons for participants to activate automatic updates were convenience and the general desire to be up to date. The online survey asked participants to rate these reasons for (de)activation of automatic updates on a 7-point Likert scale (see Table 7 in the Appendix).

3.2 Automatic Updates and Their Effect on Update Decisions

We assumed activated automatic updates would influence users in two ways: (1) that some of the users that are unhappy with automatic updates would try to avoid triggering the installation criteria for them (thereby delaying or skipping updates). This would increase participants' agency in deciding the installation time without deactivating automatic updates. (2) that users that are happy with automatic updates would slowly lose the ability to make update decisions over

time and factor in fewer potential problems before deciding. In order to find evidence for these assumptions we added two sections to our online survey.

Avoidance Behavior. On Android and iOS, automatic updates are performed by default when the phone charges and is connected to a WiFi network. For 80% of the participants the time of day that they most often charge their phone coincides with a time of day that they are usually connected to WiFi. That means that most participants are able to receive their automatic updates during the course of 24 h and do not show signs of update avoidance. Table 8 in the Appendix presents the participants' complete responses.

Effects of Automatic Update Settings. We compared the qualitative answers of participants that activated automatic updates with the answers of participants who favored manual updates. We found no qualitative differences between these groups regarding their preferred installation time and their suggested changes to the update notification. Participants who activated automatic updates mainly mentioned three concepts: (1) updates are necessary for maintenance, (2) updates are necessary for security, and (3) updates can be important without having visible effects. Only participants that favored manual updates stated that they would like to wait for experience reports from other users.

3.3 Transferring Update Behavior to Smart Consumer Devices

In an effort to understand how well the users' update behavior transfers to smart consumer or IoT devices, we start by reporting general results on the responses to update notifications shown in the online study. We present our results according to three of the six update stages discovered by Vaniea et al. [25]: deciding, preparation, and deployment. Afterwards, we elaborate on the participants' different attitudes to smartphone and smart consumer device update notifications.

Deciding. Our formative field study indicated that the participants' perception of a manual update's importance influences their decision to install them. Therefore, we asked participants to rate the importance of the presented manual update notifications on a 5-point Likert scale and provide a qualitative explanation. We present the participants' ranking of importance before going into more detail with the qualitative evaluation of the response.

Participants considered system updates the most important type of update ($m = 3.69$, $sd = 1.09$), followed by updates for cars ($m = 3.1$, $sd = 1.20$), phone apps ($m = 2.41$, $sd = 1.1$), and dishwashers ($m = 2.29$, $sd = 1.28$). Updates for shoes were considered least important ($m = 1.9$, $sd = 1.03$) of all five update notifications. Figure 1 provides an overview of the resulting scores and which group comparisons revealed significant differences. We used a one-way repeated measures ANOVA to compare the mean importance scores of the update notifications. Shapiro-Wilk's test indicated that we cannot assume a normal distribution. However, a repeated-measures ANOVA is robust against such a violation. Mauchly's test indicated that the assumption of sphericity had been

violated, therefore we report Greenhouse-Geisser corrected tests. Mean scores for the perceived importance of the update situation were statistically different ($F(3.39, 331.94) = 44.25$, $p < .001$, $\eta^2 = .33$). Table 1 shows notification comparisons with differences according to the post-hoc tests. The resulting ranking of importance indicates that participants might view smart consumer devices (that are not evidently safety-critical) to be less important than other kind of updates.

The evaluation of the open-ended questions for each update notification resulted in different themes covering the *decision* stage. Many participants reported possible positive or negative effects that they considered before updating. Amongst others, participants named new features, performance, stability, and usability improvements as potentially positive effects. Almost all of the reported negative effects were based on personal experience: participants reported that some updates removed features, introduced bugs, led to loss of personal data, and that they took too much time.

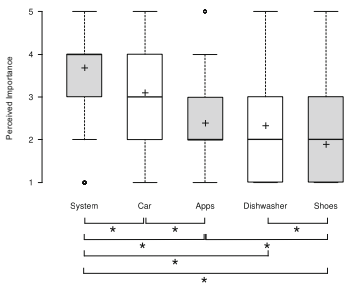

Fig. 1. Ranking of updates according to perceived importance (*) marks pairwise significant differences

Table 1. Significant differences in importance between update notifications

Comparison	Mean Diff.	Sign.	
System & Apps	1.29	<.001	***
System & Dishwasher	1.41	<.001	***
System & Shoes	1.79	<.001	***
System & Car	0.59	<.001	***
Apps & Shoes	0.51	.02	*
Apps & Car	−0.69	<.001	***
Dishwasher & Car	−0.81	<.001	***
Shoes & Car	−1.20	<.001	***

Sign. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Amongst participants with negative experience were also some who did not have any expectations from updates, but were happy if they did not impede the functionality: "if it still works afterwards, then it's fine" (P96). In the qualitative data we found three different strategies that participants used to evaluate the importance of updates:

1. *By expected changes.* Expected changes can increase or decrease an update's perceived importance. Device maintenance, new features, and security increased the perceived importance, except in cases of minor bug fixes: "probably just some bug fixes" (P74).
2. *By the presentation and content of the update notification.* Some participants scrutinized update notifications to understand the updates' importance. Participants concluded that notifications without information are not important: "the green color is a sign that it [the update] is not important" (P20) or "it did not appear to be important" (P80).

Table 2. Participants' preferred update timing.

	At notification	Later	Never	No opinion
Phone (System)	35 (38.%5)	52 (57.1%)	4 (4.4%)	–
Car (System)	40 (44.0%)	47 (51.6%)	4 (4.4%)	–
Phone (App)	32 (35.2%)	49 (53.8%)	10 (11.0%)	–
Dishwasher (System)	39 (42.8%)	24 (26.4%)	19 (20.9%)	9 (9.9%)
Shoe (System)	–	–	37 (40.7%)	54 (59.3%)

3. *By principle.* Often, participants used a general principle such as "software updates are always important" (P66) to guide their update-decisions. However, participants sometimes based their principles on the type of device, e.g., smart consumer device updates were not important, and smartphone system updates were important.

Many participants could not imagine what a smart consumer device update would change, e.g., "I can not imagine what advantages an updated dishwasher could offer" (P35). Hence, evaluating *by expected changes* might not work well with smart consumer devices. *Evaluating by notification* could work in case update notifications provide the necessary information. However, the only approach that transfers well to smart consumer devices is the last one, *by principle*. Participants applied this approach to smartphones and other smart consumer devices alike.

Preparation. Answers from the *Preparation* stage mainly concerned the update procedures' timing: delay updates in general, inconvenient update time, waiting for specific resources (power or WiFi access), or create backups before update. Participants commonly waited until bed time to install updates: "I prefer updating just before bedtime. Since I don't need a smartphone during that time." (P23).

Deployment. For the *Deployment* stage, participants wanted to decide the updates' installation time and demanded detailed information in notifications. As P62 put it: "I like having the option to decide for myself when something will be installed". More users preferred to postpone smartphone and car updates, although between 35% and 44% would update right away. The majority of participants would perform dishwasher updates right away, even though they did not regard it as especially important (ranked fourth in Fig. 1). Participants either had no opinion on the preferred time of installation or would like to skip installing the self-lacing shoes update altogether, suggesting that users do not see any benefit of updating self-lacing shoes. Table 2 shows the preferred time to perform updates.

In some cases participants did not care about small and unimportant changes and wanted to install them automatically, while still keeping the agency for important updates. In contrast, other participants preferred automatic installation of important updates: "Special updates should be installed automatically" (P65).

Comparing Update Behavior for Smartphones and Smart Consumer Devices. While participants focused on security benefits of smartphone updates (by principle), participants did not consider smart consumer device updates important by principle, probably because they did not see the point of them. Compared to smartphone updates, they focused more on safety aspects and maintenance, e.g., "Ensures that the system runs correctly" (P69 regarding car software updates). Participants focused on potential security benefits and privacy-infringements with smartphone updates, which was not a concern with smart consumer device. Most participants did not expect any visible changes to smart consumer devices after updates. Commonly, participants preferred to install smartphones updates "Instantly if WiFi is available and the battery is sufficiently charged" (P5). Additionally, some participants install smartphone updates because they are curious about potential changes, which they did not do with smart consumer devices. Participants suspected that they could not use smart consumer devices during the update process, which is why they preferred to delay updates. Participants demanded similar changes to update notification for smartphone and smart consumer device updates. However, more participants did not have design suggestions for smart consumer device update notifications, probably because they did not deem updates necessary for these types of devices.

3.4 Contradicting User Requirements

During the evaluation, we uncovered the following five different contradictions of user requirements:

CR1: Installation Time. Some participants thought updates that take a long time to install are important because they change a lot. Other participants delay these updates because they fear disrupting their regular activities. Resulting in a small conundrum: small, quickly installed, security patches may reduce the perceived importance to users – while bundling them in large updates keeps users vulnerable who defer them. This contradicting requirement is a problem for systems in immediate use such as cars or even self-lacing basketball shoes, while it is not an issue for asynchronously used smart consumer devices, e.g., dishwashers.

CR2: Amount of Information. Some participants demanded detailed update notifications that explain its purpose and affected software parts. They carefully vet updates to avoid specific negative consequences. Others did not care about information, preferred influencing the installation time, or did not want any agency. Systems may accommodate all these user types by asking them about their policy preference and adapting to their update behavior. Detailed information in update notifications is crucial for smart consumer devices since participants had difficulties understanding their purpose and effect.

CR3: UI and Changes. A few participants disliked updates that changed UIs, they claimed that older UI versions worked better and did not confuse them. Others enthusiastically looked forward to using new UIs. Hence, everyone demands information about UI changes, even though users' reaction can vary. This contradicting requirement only applies to smart devices with malleable user

interaction, such as car's touchscreens or voice interfaces. It does not apply to smart consumer devices with fixed interaction, such as the basketball shoes (only two buttons) or dishwashers.

CR4: Time of Notification. Participants could not agree on appropriate times for update notifications. Several factors influenced the appropriate installation time: (1) necessary resources (remaining battery life or internet access), (2) necessary preparations (reading the installation notes or creating a backup), and (3) when they are planning on using the device. While smartphones consider the first point, the second and third are highly context-dependent or specific to the users' update attitudes. Smart consumer device users are concerned with (3) since they want to immediately use their device (such as the basketball shoes or the car) – for these devices notification should arrive at the end of a usage session or offer to delay the installation accordingly.

CR5: Automating Updates. For several participants it was important to control updates for applications they considered important, but would even welcome automatic updates for all other applications. Other participants' approach was exactly opposite, they wanted to automatically install important updates, because they felt their decision was not necessary or beneficial in those cases. While still maintaining control for update decisions that were not critical. This contradicting user requirement applies to all IoT devices and smartphones. This issue warrants closer inspection in future work to see if those are actually opposite requirements or if participants thought about different levels of importance. Different levels of importance would result in three categories: (1) critical: automatic updates, (2) important for personal use: manual update decisions, and (3) others: automatic updates.

Interestingly, participants reported being annoyed by manual and automatic updates. Some said that update notifications requiring their decision annoyed them, which they resolved by enabling automatic updates. Others felt that updates slowed down the system or reduced the available download speed, which they resolved by disabling them. Some of those contradictions result from a fixed security policy and could be remedied by dynamic policies that are adaptable to the individual user, as suggested by Edwards et al. [4].

4 Discussion

Like all other study designs, this work and its results come with limitations. The results from our formative field study have an age bias (Table 3), our online survey' participants felt more comfortable with technology than the average population (Table 6), and both datasets have a gender bias to men. However, Amazon MTurk is more representative of the U.S. than the census-representative panel responses [19]. In the foreseeable future, the average (target) users of smart consumer and IoT devices will be older than today. Hence, more research on the security of smart consumer devices with an older population will be necessary.

Given the nature of an online survey, we collected self-reported data about update notifications that participants did not experience on their own devices.

However, we were primarily interested in the participants' update thought-process, which we could not have researched without self-reported data, even if participants experienced a real update situation.

4.1 Automatic Update Settings

The push for automatic updates by default has been effective at increasing the amount of users that keep automatic updates enabled. Previous work by Tian et al. [23] concluded that 47.7% updated their apps automatically, which has increased to 86.8% according to our results. We observed that iOS users more commonly deactivated automatic updates than Android users: 33% of them disabled automatic system updates (compared to 18% of Android users) and 16% of them disabled automatic app updates (compared to 14% of Android users). We assume that the reason for this difference is grounded in the UI: on iOS, the options to deactivate updates are in the general settings menu, whereas they are harder to find on Android. Prior to our work, we assumed that users change their update settings at most once. However, four (7.6%) participants of the formative field study stated that they had changed their update settings multiple times, indicating that the available options do not fit the participants' needs. For those users a more dynamic, context-sensitive security policy might be important [4].

We analyzed the participants' answers according to their update settings to find possible effects of those settings on the remaining manual update decisions. Participants with automatic update settings more commonly referenced concepts such as maintenance, security, and the invisibility of software-changes. We assume the reason for this difference is that users who think of the necessary but invisible changes included in updates are generally more comfortable with the idea of automatic updates. Additionally, we found that only users with manual updates wait for experience reports from other users before updating themselves. A possible explanation for this difference is that users with negative update experiences in the past are more risk-averse when installing updates. This would also explain why they deactivate automatic updates in the first place.

4.2 Transferring Update Behavior

Not all IoT device updates are automatable and some of them have minimalistic UIs, so we have to know how users will handle update decisions. Prior work [25] and our formative field study identify an update's perceived importance as a decision factor. Participants ranked the importance of the five update notifications as follows: operating system updates, car, apps, dishwasher, shoes. Indicating that users might think IoT device updates are less important than other kinds of updates, except for safety-relevant IoT devices.

In our qualitative data, we found three different approaches to evaluate the importance of updates: by the expected changes, by the presentation or content of the update notification, or by principle. We discovered that participants in our study could often not imagine what kind of changes updates for IoT devices

might entail. However, some users judge the importance of an update by evaluating the expected changes, impacting their install decision.

One of the root causes for this could be the analogical transfer of update behavior based on the term 'update'. An 'update' often implies new and improved software, which either scares or excites users. In recent years, we saw how major updates with invisible changes are bundled with minor visible changes, such as dark mode[1], or a new set of emojis, to communicate the update's importance. Analogical transfer of update decisions from smartphones to IoT devices may cause similar expectations. Son et al. [22] discussed how words influence the analogical transfer of concepts. Renaming 'updates' for IoT devices may avoid expectations of visible changes. Participants often mentioned 'maintenance', e.g. P43 "So that I can use the device without problems". We suggest this term for IoT updates that (1) do not contain visible changes and (2) cannot lead to loss of data. We do not recommend a name change for other updates to avoid undermining users' trust. Separating the terms "updates" and "maintenance" could eliminate unwarranted expectations of visible changes and reduce the fear of unexpected functionality or user interface changes.

More than half of the participants would have delayed the updates for the smartphone or the car which is in stark contrast to the update for the dishwasher or shoes. We think that this is a sign of risk-aversion, since the participants heavily rely on the functionality of those devices. While this study focused on smart consumer devices used by individuals, there is also communal use of smart consumer and IoT devices. While we expect increased risk-aversion in these cases, future research would be valuable to get a more complete picture of users' update preferences. The most popular option for the dishwasher update was to install it at the time of the notification, presumably as the distraction from the main task was perceived as less severe and participants had no issues with postponing an unattended task. Regarding the updates for shoes, participants either had no opinion about their preferred time of installation or did not want to install them at all. We interpret this as a sign that participants did not see the point of self-lacing shoes in general and did not want to maintain them in a working condition.

Comparing participants' perspective on updating smartphones and IoT devices also warrants a discussion about differences between devices and applications: (1) if the device has a fixed user interface or a reconfigurable one, (2) if the device is for a single purpose or for multiple purposes, (3) the type and amount of available resources such as Internet connection and power supply, and (4) how frequently people use them in everyday life. Comparing along these categories suggests that smartphones and IoT devices have different usage patterns - an exception being multi-purpose IoT devices with a malleable user interface such as voice assistants. If we instead compare specific IoT and smartphone applications it makes sense to classify according to user-centered themes from the qualitative analysis: urgency of use, importance of continued functionality, importance of

[1] Dark mode changes the UI to a darker color palette to reduce strain on the eyes in low ambient light.

specific feature-set, and importance of personal data associated with application. Especially the first two themes are important factors for smartphones as well as IoT devices and they will shape users' update decisions. However, we should not overestimate the usage patterns specific to applications or devices, since decisions for new devices or applications are often based on prior experience with other applications [26].

User interaction design is a tool for communication between users and the underlying technology. It should take the users' mental models into account and translate them as well as possible to corresponding mechanisms. Our findings can serve as a basis to understand user-specific constraints on update procedures. This gives several design indications which we will present in the next section. The technical goal of broadly deployed updates for security and maintenance purposes does not seem far-fetched and does not necessarily contradict users' values.

4.3 Implications for Design

Users consider several types of information before installing updates: how important they perceive the update, if they update interferes with their current primary task, and if they can live with the expected changes. How users perceive those factors can be influenced to some degree by design mechanisms. In the following, we provide a series of design implications based on the open-ended questions in our online survey to lay foundations for future work. In future work, we plan to expand and validate these recommendations.

ID1: Store information about users' software or IoT device usage and use this data to adapt update procedures to them. A common sentiment among participants was that they only consider apps that they frequently use as important and worthy of updates. This allows auto-updating IoT devices (if possible) or smartphones apps that user do not consider important without infringing on their sense of control.

ID2: Reduce the amount of update notifications as much as possible. Participants considered frequently occurring updates as not interesting and unimportant. In contrast, they perceive rare updates as special and probably important enough to warrant their attention. This applies to IoT devices and smartphones equally.

ID3: Important updates should take longer to install than unimportant ones. Participants perceived large updates that take longer to install as more important than quickly installed updates. Hence, the duration of the installation should reflect the update's importance. In most cases, developers should consider an update important if it reflects the users' values of important updates (this requires some feedback from individual users). However, systems should be able to (if possible) install critical updates that do not impact user experience without user-interaction. This applies equally to IoT devices and smartphones. However, immediate use is important for some types of IoT devices (e.g., the car, shoes, TVs, ...) the timing of these longer updates is critical.

ID4: Restrict install options for important updates to convey importance. The interface options available in the update notification also communicate how important an update is. As one participant phrased it: "Since I can delay the update, it is apparently not an important update" (P53). This type of modifications has even more effect on IoT devices with immediate use requirements, since an update has to be very important to force active waiting until the update is finished. Other devices, such as a dishwasher or apps that are not used often, will not be as affected as much by such a design change.

ID5: Clearly communicate possible consequences of an update. The fear of data loss made our participants delay an update until they create a backup of their data. Informing users if their personal data will be affected by the update and creating automatic backups could reduce the users' fear of updating. Participants were worried that an update could take longer than expected and prevent them from completing their primary task. Therefore, it is important that the update notification conveys these aspects ahead of time. This is important for software and devices that users depend on for regular activities that cannot be arbitrarily delayed: software required for work related tasks, and mobility devices (cars, shoes).

ID6: Provide context-dependent options to delay installation time. One of the major suggestions of improvement for update notifications was that users want more agency to select the time of installation. Some participants proposed a "later" button, some wanted to select a certain time, and one suggested an option "install after current task". We suggest decoupling the decision time from installation time in a context-sensitive way to provide a user-centered installation time. All software and devices that users immediately require and that are task-centered would benefit from such an option. Distinguishing tasks might be easier for IoT devices even (as in all our presented IoT devices), since they are often only used for a single purpose.

ID7: Changes of the User Interface should remain optional wherever possible. Updated user interfaces were considered unimportant by most participants. Some considered UI changes a burden, others thought they had the potential to make them feel as if they had gotten a new device. Since UI updates could be a barrier to updating, those should be separated from the rest and remain optional for users. This design would probably not affect IoT devices as much, because many of them do not have a malleable user interface in the first place. However, this could be a necessary option for devices that are controlled by a touch screen or voice.

ID8: Let users decide if software that they consider important should update automatically. Some participants were annoyed by the amount of updates that they considered unimportant: they wanted to have these automated but still manually update apps they consider important. Other participants thought it did not make sense for them to be able to decline important updates, instead they were willing to decide upon less important updates. Especially for smartphones a choice like this could severely improve the amount of update notifications that users see, while increasing the relevance of these notifications.

This distinctions is less important for IoT devices, because they receive a smaller amount of updates in general.

5 Related Work

Reasons for (Not) Updating. Vaniea et al. [25] found that participants who always installed updates or believed in an update's importance readily installed updates, whereas participants who were satisfied with current versions delayed updates. Satisfaction with the current software version, undesired UI changes, the perceived lack of purpose of software updates, and negative prior update experiences hinder participants from updating [26]. Mathur et al. [15] found that 40.5% of participants thought about the costs of updating, 29.2% considered the necessity of updates before installing, and 7.5% were concerned about the potential risk of updating. We extend Mathur et al.'s work with a focus on smartphones and smart consumer devices.

Users' main source of information about updates is the notification that they see. Users often misunderstand how updates change their system, which frustrates them and about 16% of them refuse to apply updates [5]. Tian et al. [23] found that 42.6% participants regretted updating a smartphone app in the past because of bugs, "bad" UIs, and privacy-invasive practices. Since participants relied on reviews for their update-decisions, the authors introduced a review-based support system. Mathur et al.'s [14] formative study found that users want know about an update's purpose and that trust in vendors, expected compatibility issues, user interface changes, social influences, and installation time affected update decisions. They built a prototype of a corresponding OS update process which satisfied half of the participants because it decreased interruptions.

Effects of Automating Updates. According to Marthur et al. [13], users are comfortable with auto-updating apps if they consider them important, trustworthy, or if they are satisfied with them. Previous negative experience with updates reduces users' comfort with auto-updating. Edwards et al. [4] finds that removing users from security choices creates a problem when automation fails: users are ill-equipped to understand and cope with security decisions. Wash et al. [27] found that users misunderstand their own update behavior, which is bad since future update decisions are based on wrong assumption, which improved education cannot fix. They argue that removing users from most decisions makes it difficult for them to intelligently make the remaining decisions. Worryingly, there is some indications that users transfer their expectations from one system to another, e.g., Ponticello et al. [17] found participants who transfer their authentication expectations. The same could hold true for users' update expectations and decision strategies. Forget et al. [7] found that users with misaligned estimated and actual security expertise might make rational decisions that lead to ineffective security. Hence, user engagement which might lead to risky decisions in these cases.

Updating IoT Devices. Fernandes et al. [6] found that over 55% of existing SmartApps on SmartThings are over-privileged and have inadequate security controls. Zeng et al. [28] used an exploratory design study to understand users' requirements for access control in multi-user smart home designs. In 2006, Bellissimo et al. [1] found that secure updates for IoT devices face challenges such as untrusted infrastructure, sporadic network connectivity, or limited local resources. Simpson et al. [21] discuss usability challenges of applying updates on IoT devices, specifically update notification and predicting convenient update times.

6 Conclusion and Future Work

Among other things, we found that the prevalence of automatic updates for applications on mobile phones has increased to 86.8% (in comparison to 47.7% [23]) and that 18.7% of participants deactivated automatic system updates. Our results suggest that iOS users deactivate automatic updates more often than Android users. We hypothesize that easy access to the relevant option in the UI explains most of that difference (see Sect. A). Users explained their deactivated automatic updates with a fear that updates might introduce flaws and agency in update decisions, fear of compatibility issues, and a limited or expensive data plan. The most important reasons to activate automatic updates were staying up to date, convenience, and security. We expected to find evidence of avoidance behavior amongst participants (i.e., avoiding charging their phone while connected to WiFi), but our results do not support this. Participants who enabled automatic updates approached update decisions similar to those with manual updates. However, three concepts were more important to them: the idea that updates are necessary for maintenance, for security, and that updates could be important even if they do not have any visible effects. Additionally, participants who favored automatic updates were not interested in other users' experience reports.

Prior work [25] and our formative field study provide evidence that the perceived importance of an update is a decisive factor for installing it. Our results indicate that users perceive updates for smart consumer devices as less important than regular updates, except for safety-relevant devices. Our contribution includes a classification of how users evaluate the importance of updates: by expected changes, by the presentation and content of the notification, and by principle. Participants in our study could not imagine meaningful changes for smart consumer devices; the corresponding notification lacked information. Therefore, the evaluation by principle is the only method that led participants to conclude that updates for these devices are important and that they would install them soon or immediately after receiving the notification. Prior work [22] indicates that a concept's name promotes analogical transfer: An 'update' might imply new features or at least focus on visible changes. However, in the case of IoT device updates, participants mentioned the concept of 'maintenance' more often. We hypothesize that using the word 'maintenance' to describe updates

without visible changes might increase users' willingness to install them. We provide a list of areas of tension based on conflicting motivations and themes from our data. These open up new directions for designing update solutions that work well for everyone.

At the workshop, participants discussed areas of future research with us. The first idea was identifying and developing a fine-granular terminology to describe the exact nature of updates. Using such terminology, developers could easily communicate updates' effects to end users – simplifying their update decision. The second idea concerned how the companies who create software updates manage this process. Understanding the rationale for changing user interfaces, deprecating features, packaging update bundles, and automating update decisions may help in improving end users' update experiences.

A Instructions on Finding Update Settings

A.1 Android

Operating System Updates: (1) Check if developer options are activated - until version 8.x they are found at the bottom of the main settings menu. From version 9 they are found in the system settings menu; (2) If developer options are activated and the corresponding menu exists: check if "Automatic System updates" are activated (default) or not.

Application Updates: (1) Open your Google Play Store Application; (2) Tap the hamburger-menu in the upper-left corner to open the Play Store menu; (3) Scroll down to the settings option; (4) Tap on the option "automatic updates".

A.2 iOS

Operating System Update: (1) Open the iOS settings; (2) Scroll down to the option "General" and tap it; (3) In this menu the entry "Software update" should be in the second place; (4) Wait for the listing to load, the option for automatic updates should be at the bottom of display.

Application Updates: (1) Open the iOS settings; (2) Scroll down and choose the option "iTunes & App Store"; (3) Below the heading "Automatic Downloads" there is an option for applications; (4) A green button shows that automatic downloads are enabled, and a grey button shows that they are not.

B Formative Field Study: Questionnaire

- **Update Settings:**
  (1) Which operating system and which version is currently installed on your phone? (2) What is your current setting for automatic operating system updates? (3) Why did you choose this setting? (4) What is your current setting for automatic application updates? (5) Why did you choose this setting?

– **Demographic data:**
(6) What is your gender (female, male, diverse, I prefer not to answer)? (7) How old are you? (8) What is your major (for students) or what is your occupation (for non-students)? (9) Please tell us how well the following statements apply to you (1 = Not at all ... 7 = Very much): (a) It is difficult for me to convince computers to do what I want. (b) Concerning computers, I don't think I am very competent. (c) I think I am a skilled computer user. (d) I can help others with their computer problems. (e) I find it difficult to learn new computer software. (f) I am able to learn a programming language. (10) Provide three things that you regularly do in order to keep your smartphone or your personal data secure.

Table 3. Participants' demographics in the formative field study

	#	m	sd
N	52		
Age		23.62	3.71
Self-Efficacy (all)		5.21	1.26
Self-Efficacy (w/out students)		4.88	1.27
Gender			
Women	13		
Men	37		
Preferred not to say	2		
Students	45		
Computer Science	13		
Business	8		
Teaching	7		
Law	6		
Psychology	4		
Other	7		
Non-students	7		

C Formative Field Study: Demographics, Codebooks, and Update Settings

– **Reasons for OS update settings:**
Do not remember (18); Maintain control over installed software (2); General desire to be up to date (2); Installed OS does not provide automatic update option (2); Practicality (1); Compatibility problems (1); Data cap on their mobile contract (1); Security (1)

– **Reasons for application update settings:**
Did not change it (15); Maintain control over installed software (8); Data cap on their mobile contract (7); Practicality (4); Annoyance (4); Do not remember (4); General desire to be up to date (2); Installed OS does not provide automatic update option (2); Not enough storage space (1); Security (1)
– **Security-relevant day-to-day behavior:**
Authentication (23); Self-Denial of potentially useful products or features (18); Check data protection specific settings (16); Password management (10); Secure network access (10); Backup (7); Use common sense (7); Protection software (6); Encryption (4); Physical access control (4); Updates (4); Others (4)

Table 4. Distribution of OS and application updates for Android and Apple users.

	OS updates		Application updates	
Apple	On:	**17**	On:	**15**
	Off:	**6**	Off:	**10**
Android	DO on/Updates on:	**3**	Always:	**1**
	DO off/Updates off:	**1**	WiFi only:	**21**
	DO off/Updates on:	**16**	Never:	**3**
Total		**43**		**50**

Annotations. Number of participants that chose the possible option. DO = Developer options.

Table 5. Distribution of OS and application updates regarding self-efficacy.

OS version	Self-efficacy $\geq$ **4**				Self-efficacy $<$ **4**			
	OS updates		App updates		OS updates		Application updates	
Apple	On:	**4**	On:	**14**	On:	**1**	On:	**1**
	Off:	**16**	Off:	**8**	Off:	**2**	Off:	**2**
Android	DO on/Updates on:	**3**	Always:	**1**	DO on/ Updates on:	**0**	Always:	**0**
	DO off/Updates off:	**1**	WiFi only:	**13**	DO on/Updates off:	**0**	WiFi only:	**8**
	DO off/Updates on:	**11**	Never:	**3**	DO off/Updates on:	**5**	Never:	**0**

Annotations. Number of participants that chose the possible option. DO = Developer options.

D Online Survey: Questionnaire, Demographics, Reasons for (De)activation, and Update Avoidance Behavior

1. **Update settings on your smartphone:**
   (a) Which OS do you use on your smartphone? [Android, iOS, other]; (2) Which exact version of the chosen OS do you use?; (3) Take a screenshot of your OS update settings and upload it; (4) Have you changed those settings in the past?; (5) Why did you choose this setting? (6) Take a screenshot of your app update settings and upload it; (7) Have you changed those settings in the past?; (8) Why did you choose this setting?
2. **Personal expectations about updates:**
   For all update notifications shown in Sect. E*:* (1) You are just about to use (insert device here) and the following update notification pops up; (2) How important do you think is this update? [5-point Likert scale]; (3) State your reasons for the last answer; (4) What kind of changes would you expect from such an update?; (5) When would you update? [Now, Later, Never]; (6) State your reasons for the last answer; (7) How would you change the update notification?
   Afterwards: (1) How large do you think is the share of app updates that are relevant for security? (2) How large do you think is the share of OS updates that are relevant for security? (3) How should an update be presented so that you perceive it as security-relevant?
3. **Reasons for (de)activation of automatic updates:**
   (1) Other people gave the following reasons for their activation of automatic updates. Please state how much you agree with them [5-point Likert scale]: I want to keep up with the current version, It is convenient to have them done automatically, Installing updates is good for security, I am annoyed by notifications in case of manual update installation, other; (2) Other people gave the following reasons for their deactivation of automatic updates. Please state how much you agree with them [5-point Likert scale]: I want to control which software and which version is installed on my phone, I fear compatibility problems with other software, my phone contract includes a low amount of data, I am annoyed by automatic updates, My phone does not have enough free storage for updates, others.
4. **Update avoidance behavior:**
   (1) At what time of day do you charge your phone battery?; (2) At which location do you usually charge your phone battery?; (3) At which locations is your phone usually connected to a WiFi network?; (4) At which times of the day is your phone connected to the WiFi, so that automatic updates could be installed?
5. **Personality:**
   (1) Psychological Reactance Scale [Hong et al. 1996]; (2) Affinity to Technology scale; (3) Big Five Inventory scale [Agreeableness and Conscientiousness]
6. **Demographic data:**
   (1) Gender; (2) Age; (3) How would you rate your knowledge of German?;

(4) Type of occupation; (5) Field of occupation; (6) Highest completed educational level; (7) Available household-income per month

7. **Comments:**
   (1) Did you experience technical problems during this questionnaire?; (2) Please describe your problems; (3) General comments

E Online Survey: Update Notifications

We showed participants five update notifications: (1) Figure 2 shows a system update, (2) Figure 3 shows several available application updates, (3) Figure 4 shows an open dishwasher that displays a notification of an ongoing update, (4) Figure 5 shoes an available update for self-lacing basketball shoes, and (5) Figure 6 shows an available update in a car.

F Online Survey: Codebook

- **Curiosity (11)**
- **Update Preparation** after relevance check (11), Update as soon as electricity and/or internet available (84), use own WiFi (6), Prevention of data loss [after Backup (15), Threat of data loss intimidating (9)]

Table 6. Participants' demographics in the online survey

	#	m	sd
N	91		
Age		29.13	8.39
Affinity for technology interaction scale		4.56	0.95
Reactance to autononmy scale		2.85	0.59
Big five inventory scale			
Extraversion		2.90	0.36
Agreeableness		3.52[a]	0.57
Conscientiousness		3.51[a]	0.49
Neuroticism		3.15	0.39
Openness to experience		2.69	0.55
Gender			
Women	16		
Men	73		
Preferred not to say	2		

[a]The above average scores for conscientiousness and agreeableness are noteworthy, since they correlate with increased security awareness [9].

Table 7. Ranked reasons for (de)activing automatic updates

Reasons for deactivation	m	sd
I want to control which software (version) will be installed	4.45	1.82
My phone contract has a limited data cap	4.09	2.11
I am concerned about potential compatibility problems	3.47	1.74
I am annoyed by automatic updates	3.46	2.01
My phone has insufficient storage space for updates	2.97	1.9
Reasons for activation		
Security reasons	5.49	1.41
"Stay up to date"	5.19	1.54
Convenience	5.14	1.68
Annoying update notification	4.62	1.79

Table 8. Participants who avoid charging their battery and connecting to WiFi at the same time might demonstrate update avoidance behavior

	Morning	Before noon	Noon	Afternoon	Dinnertime	Night	Whenever necessary
Charge battery	5	4	0	3	8	68	4
WiFI[a]	40	36	27	0	55	75	

[a]Multiple choice response

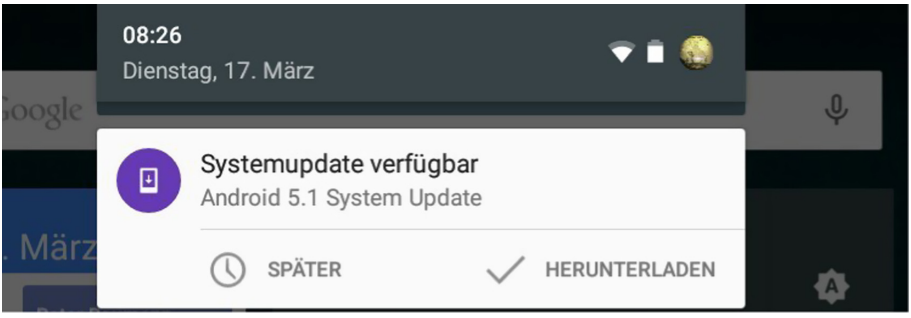

Fig. 2. Android system

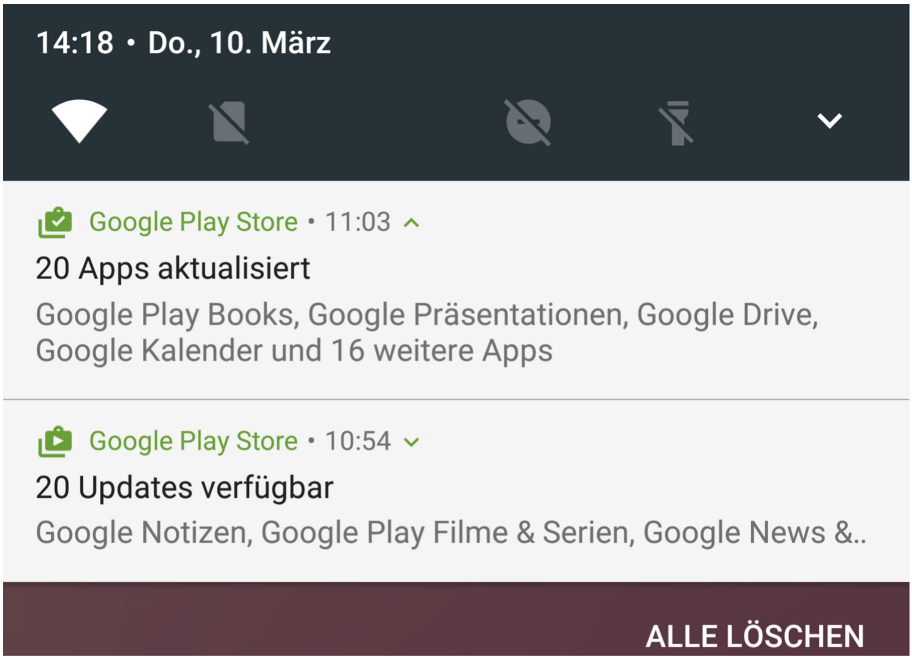

Fig. 3. Android app

- **Scheduling** Time for Update [Immediately (61), At next opportunity (116), Point in time of no importance (11), No time for Updates (22)], Update prevents use (150), not while out and about (25), Not leave pending/remove notification (42), no counter-argument apparent (9), No disruption because in background/finished quickly (40), App Updates do not disrupt use (15)
- **Scepticism** IoT incomprehension (99), Incomprehension (40), no demand/unimportant (95), New devices error-prone (3),
- **Principles of importance** Update size implies importance [Small changes are unimportant (7), Update important if finished quickly (2), Bigger Update → later, smaller → sooner (3), Important because of long installation duration (1), System Updates take longer (7)], Rare Updates important (16), Updates are important (113), System updates are important (79), Update only important for used apps (63), Apps differ in importance (2), important → sooner (20), Updates unimportant for IoT devices (133)
- **Expected changes** User Interface [UI Changes (75), Device in mint condition through update (3), Updates important for UX change (2), Improved Usability (27)], No noticeable changes (244), Maintenance (185), Bug-fixing (290), New features (252), Improvements (114), Performance (198), Changes anticipated by users (4), Safety (59), Privacy (8), Security (338), (only) devices attached to network need be up-to-date (3)

Fig. 4. Dishwasher

- **Negative Experiences** Never change a running System (51), Wait for field reports (11), Updates can cause errors (17), No update because of space lacking (2), Negative experience long duration (2), Negative experience as reason without explanation (7)
- **Update Deployment** Right to a say [Choice to delay makes update unimportant (4), Right to a say desired (49), Choice when to install update (25)], Information through notification [Notification no boost to confidence (10), Improved update notification (58), visual information within notification (32), More information within notification (349), Notification emphasizes importance (2), Notification as source of information (16), Less information within notification (49), Notify through phone (4)], Automatic updates [Automatic updates preferred (48), Unimportant updates should happen unsupervised (6), Critical updates automatically (22)], Timing of notification disruptive (14), Timing of notification convenient (1), Download vs. installation of update (4), No suggestion (529).

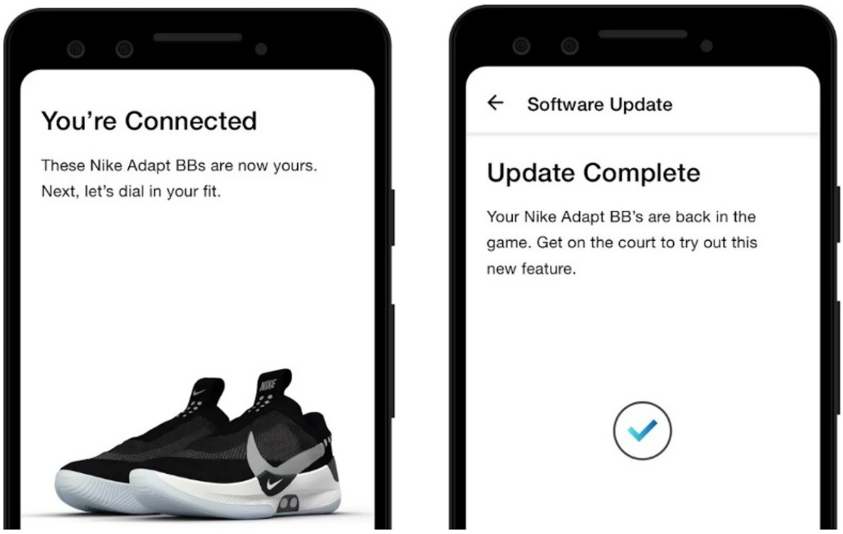

Fig. 5. Basketball shoes

Fig. 6. Car system

References

1. Bellissimo, A., Burgess, J., Fu, K.: Secure software updates: disappointments and new challenges. In: 1st USENIX Workshop on Hot Topics in Security, pp. 37–43 (2006)
2. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qual. Res. Psychol. **3**(2), 77–101 (2006)

3. Duebendorfer, T., Frei, S.: Why silent updates boost security. TIK 302, ETH Zürich (2009)
4. Edwards, W.K., Poole, E.S., Stoll, J.: Security automation considered harmful? In: Proceedings of the 2007 Workshop on New Security Paradigms - NSPW 2007, p. 33 (2008)
5. Fagan, M., Khan, M.M.H., Buck, R.: A study of users' experiences and beliefs about software update messages. Comput. Hum. Behav. **51**, 504–519 (2015). https://doi.org/10.1016/j.chb.2015.04.075
6. Fernandes, E., Jung, J., Prakash, A.: Security analysis of emerging smart home applications. In: 2016 IEEE Symposium on Security and Privacy (SP), May 2016
7. Forget, A., et al.: Do or do not, there is no try: user engagement may not improve security outcomes. In: Proceedings of the Twelfth Symposium on Usable Privacy and Security (2016)
8. Franke, T., Attig, C., Wessel, D.: A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. Int. J. Hum.-Comput. Interact. **35**(6), 456–467 (2019). https://doi.org/10.1080/10447318.2018.1456150
9. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A.: Correlating human traits and cyber security behavior intentions. Comput. Secur. **73**, 345–358 (2018). https://doi.org/10.1016/j.cose.2017.11.015
10. Hong, S.M., Faedda, S.: Refinement of the Hong psychological reactance scale. Educ. Psychol. Measur. (1996). https://doi.org/10.1177/0013164496056001014
11. Ion, I., Reeder, R., Consolvo, S.: "... No one can hack my mind": comparing expert and non-expert security practices. In: Proceedings of the Eleventh Symposium on Usable Privacy and Security (2015)
12. Li, F., Rogers, L., Mathur, A., Malkin, N., Chetty, M.: Keepers of the machines: examining how system administrators manage software updates. In: Proceedings of the Fifteenth Symposium on Usable Privacy and Security (2019)
13. Mathur, A., Chetty, M.: Impact of user characteristics on attitudes towards automatic mobile application updates. In: Proceedings of the Thirteenth Symposium on Usable Privacy and Security (2017)
14. Mathur, A., Engel, J., Sobti, S., Chang, V., Chetty, M.: "They keep coming back like Zombies": improving software updating interfaces. In: Proceedings of the Twelfth Symposium on Usable Privacy and Security (2016)
15. Mathur, A., Malkin, N., Harbach, M., Peer, E., Egelman, S.: Quantifying users' beliefs about software updates. arXiv (2018). https://doi.org/10.14722/usec.2018.23036
16. van der Meulen, R.: Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. https://www.gartner.com/en/newsroom/press-releases/2015-11-10-gartner-says-6-billion-connected-things-will-be-in-use-in-2016-up-30-percent-from-2015
17. Ponticello, A., Fassl, M., Krombholz, K.: Exploring authentication for security-sensitive tasks on smart home voice assistants. In: Proceedings of the Seventeenth Symposium on Usable Privacy and Security (2021)
18. Rammstedt, B., John, O.P.: Kurzversion des big five inventory (BFI-K): Diagnostica **51**(4), 195–206 (2005). https://doi.org/10.1026/0012-1924.51.4.195
19. Redmiles, E.M., Kross, S., Mazurek, M.L.: How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples. In: 2019 IEEE Symposium on Security and Privacy (SP) (2019)

20. Reeder, R.W., Ion, I., Consolvo, S.: 152 simple steps to stay safe online: security advice for non-tech-savvy users. IEEE Secur. Priv. **15**(5), 55–64 (2017). https://doi.org/10.1109/msp.2017.3681050
21. Simpson, A.K., Roesner, F., Kohno, T.: Securing vulnerable home IoT devices with an in-hub security manager. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (2017)
22. Son, J.Y., Doumas, L.A.A., Goldstone, R.L.: When do words promote analogical transfer? J. Probl. Solving **3**(1) (2010). https://doi.org/10.7771/1932-6246.1079
23. Tian, Y., Liu, B., Dai, W., Ur, B., Tague, P., Cranor, L.F.: Supporting privacy-conscious app update decisions with user reviews. In: Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (2015)
24. Tiefenau, C., Häring, M., Krombholz, K.: Security, availability, and multiple information sources: exploring update behavior of system administrators. In: Proceedings of the Sixteenth Symposium on Usable Privacy and Security (2020)
25. Vaniea, K., Rashidi, Y.: Tales of Software Updates: the process of updating software. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (2016)
26. Vaniea, K.E., Rader, E., Wash, R.: Betrayed by updates: how negative experiences affect future security. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (2014)
27. Wash, R., Rader, E., Vaniea, K., Rizor, M.: Out of the loop: how automated software updates cause unintended security consequences. In: Symposium on Usable Privacy and Security, pp. 89–104 (2014)
28. Zeng, E., Rösner, F.: Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In: Proceedings of the 28th USENIX Security Symposium (2019)