JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2020, 1–22
doi: 10.1093/cybsec/tyaa017
Research paper

Research paper

An analysis of perceptions and support for Windows 10 Home Edition update features

Jason Morris[1], Ingolf Becker [2]* and Simon Parkin[1]

[1]Computer Science Department, University College London, Gower Street, London WC1E 6BT and [2]Computer Science Department, University College London, Gower Street, London WC1E 6BT

*Correspondence address. Department of Security and Crime Science (SCS), University College London, Gower St, WC1E 6BT. E-mail: i.becker@ucl.ac.uk

Received 30 June 2020; accepted 21 August 2020

Abstract

Home computer users are regularly advised to install software updates to stay secure. Windows 10 Home Edition automatically downloads and installs updates, restarting the computer if needed. Automatic restarts can be managed through a number of features, such as 'active hours' (within which a computer will not restart to complete an update) or by setting a time for restart. Applications active prior to a restart can register with the operating system, to automatically restart once updates have been installed. This research investigates if the features Microsoft provides for managing updates on Windows 10 Home Edition are appropriate for computer owners. We build a model of Windows 10 update behaviour, identifying interaction points between update features and users. We contrast theory with reality in a survey with 93 Windows 10 Home users, capturing experiences and perceptions. While overall perceptions of updates were positive, the pattern of use of most participants was incompatible with the default 'active hours' settings (28% of participants knew of its existence). Participants were mostly unaware of quality (bug fix) updates, mostly perceiving that updates add features. Half of our participants reported unexpected restarts, while half also reported growing concern about the state of their device if an update took a long time. Those with previous negative update experiences had weaker beliefs about their ability to control updates than those who had not. To make the updates less disruptive, applications can request to be restarted by Windows after a reboot. Of the 47 commonly used applications which were tested, only two supported seamless continuation after a restart. Unsaved data were lost in 21 applications, and 14 appeared to rely on internal autosave features to capture unsaved data, but did not completely restore User Interface arrangements. We recommend that operating systems obtain explicit permission for restarts, consistently; there are opportunities for features such as active hours and update progress displays to learn from usage activity. At the same time, applications should be more resilient to restarts to reduce the burden on users to recover their activities.

Introduction

A key piece of information security advice given to users by both government organizations and security practitioners is to install operating system and software updates as soon as they become available. Doing so is seen as the way to eliminate vulnerabilities, towards creating a safer computing environment for the user, more so if done in a timely fashion [1]. The concern is that while vulnerabilities remain they could be exploited by attackers, who may have ready access to tools that allow them to target users of popular operating systems indiscriminately.

Software producers have, in some cases, automated the update process, in an effort to make it easier for users to have up-to-date software. This approach is not without drawbacks; software that is downloading or installing updates has the potential to interrupt a

user's tasks. In terms of the risks of updates, if an update was to fail (or otherwise break existing functionality), it could cause prolonged or irreparable availability issues. Similarly, an update might change a familiar user interface or feature, putting the user in the unexpected situation of needing to relearn how to use some aspect(s) of their software. As user software portfolios grow over time, these costs and risks grow proportionately with them [2].

Users may act to postpone updates or not think they are a concern [3]. Software producers can also now be seen to automate updates so that they can be scheduled and rescheduled, but not avoided indefinitely. The entry-level version of Windows 10, 'Home Edition' (released in July 2015), removed the ability of users to turn automatic updates off. This version of Windows 10 downloads and installs updates as soon as possible, scheduling an automatic restart within 24 h (if required) to complete the installation. This includes bringing the system out of standby, if necessary. The user is notified of the scheduled restart, but unable to cancel it. As an operating system provides an execution environment for many applications, an operating system restart has the potential to disrupt other running applications. If work is in progress and cannot be saved, a reboot will lead to a loss of data. Even if data can be recovered, there is an obvious disruption to active applications and their operating state, compounding the potential impact of the approach.

We examine existing research on the challenges of updates for users. We then present a model of the update behaviour of Windows 10 Home Edition and explore user perceptions of specific features and behaviours of the operating system's update features. We use the model to highlight the interactions users have with the system, and the potential consequences of these interactions for the user should they be misconfigured. We contrast this model with user experiences, through an online survey with 97 UK Windows 10 Home users. From our findings, we see that the default setting of the main feature to control when updates are installed – *active hours* – is unsuitable for the majority of our participants and the way they use their devices and that 72% of participants were not aware of the feature. Emphasizing these findings, approximately half of the participants reported restarts as being unexpected.

Windows offers applications the ability of a managed closure and subsequent restart after Windows has updated. This means that in principle Windows restarts can be non-disruptive in instances where the user is not present We find that only 2 of 47 commonly used applications fully support this seamless recovery, emphasizing that there are residual costs to the user when a system is restarted for updates. We close with discussion and conclusions.

Background and related work

Motivating the need for software updates

Software may be released that has faults. Features may be changed, or new ones added over time, which may also have faults. These faults may be exploited by malicious parties to access and manipulate a computer. This affects home users and organizations alike. To address these faults, software producers create software security updates or patches that, once applied to a machine, are assumed to eliminate a vulnerability from that machine. By way of an example, during 2017 Microsoft released 681 security updates across their product range.

Vaniea [4] describes security updates as 'unsolved, solved problems'. This refers to the principle that a vulnerability for which a security update exists should not be considered 'solved' until the relevant security update is applied to all machines that it needs to be applied to. Indeed, applying security updates in a timely manner is necessary to reduce the window of exposure of a vulnerability.[1]

Zero-day vulnerabilities are an extreme example of where details of an exploit become widely available before a software update exists to mitigate it. There is then a sense of software producers needing to create security updates quickly. Conversely, for updates to be effective, the expectation is that they are applied to end user machines quickly [1]. Where security updates should typically be invisible to users, feature updates are not. These may add new functions and features, where there is an argument to separate them from security updates [4, 5] (which to date is not happening consistently). Feature updates may change functionality or the user interface, necessitating changes to users' ways of working.

The potential for updates to bring problems of their own, be it faults or unexpected (and potentially unwanted) changes, may dissuade users from applying a security update [6]. Updates are perceived as unnecessary, unimportant and consuming a lot of data, while taking a long time to install, requiring restarts and occupying large disk space, and leaving users facing risks of potentially malicious updates and data loss [7]. Users may have dozens of software packages on their machines, from multiple vendors, each communicating updates and the need to update that software [2]. In this context, the rejection of advice to 'install the latest software and app updates' may then appear to be a rational approach [8]. Automation is a means to alleviate some of this burden, but even here different approaches to automation – such as automated 'silent' updates or a one-click update process – can vary in their success [9, 10].

The need for human control

Automatically installing software updates minimizes the window of opportunity for vulnerabilities to be exploited. Where updates require a device or software restart, consideration must be given to both the direct cost of disrupting users' primary tasks, and the indirect costs of reducing users' opportunities to observe, understand and ultimately work with the automated update mechanism.

Existing research within organizations tells us that users have a limited budget for complying with security demands [11]. The notion of a limited budget for security has broader applicability to home users too [8, 12]. A user's 'compliance budget' must be spent wisely by software providers, or a user may act instead to reduce the perceived burden, most directly by ignoring or working around security expectations. This may explain the plethora of online forum posts and magazines providing unofficial advice on how to disable automatic software updates. This can range from reconfiguring readily accessible features (e.g. marking a network connection as 'metered'), to high risk, specialized changes, such as manually editing the operating system registry. Dedicated software solutions have also emerged, which can continuously adjust the 'active hours' period to include the current time [13], or automatically enable and disable Windows update services as required [14].

Users who lack understanding of the update mechanism are less likely to be able to identify and troubleshoot problems [15]. A non-functioning update mechanism suggesting to 'search the web' (see Fig. 1) alongside an eight-digit, hexadecimal error code may not support a clear path to resolution for a non-expert user.

It has been widely established that changes to features and interfaces are common reasons for not updating, especially if there have

1 The day after Microsoft's 'Patch Tuesday' has been labelled 'Exploit Wednesday' to reflect this race.

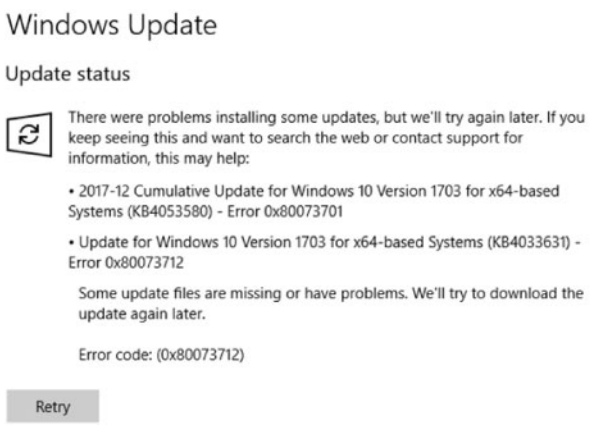

Figure 1: Screenshot of Windows update messages when updates fail.

been previous negative experiences [2, 6, 16–18]. Bergman and Whittaker [16] explained the impact of changes to interfaces in terms of five key cognitive concepts: a loss of cognitive automation (a need to reassess the interface, taking attention away from a task); negative transfer effects (the need to discard knowledge of 'doing things the old way'); rebuilding cognitive maps (such as rediscovering where features are); the need to retrain procedural memory; and the demotivating effects on the user of a feeling of loss of overall control.

Wash *et al*. [15] examined the Windows 7 Update process, which allowed users to configure the degree of update automation for key update stages. Users' intentions were compared to what the system was doing in reality (combining user engagement with log analysis). The authors found a discrepancy between actual and expected behaviours for the majority of their participants, suggested as being a result of 'removing users from the loop'. Farhang *et al*. [19] examined the upgrade practices and perceptions of Windows users as they choose whether to upgrade to Windows 10. They make four practical design recommendations for operating system producers to address the issues identified by their survey study. These were improved communication to address privacy concerns of windows updates, better upgrade messaging, improved management of security after the end-of-life and reduction of perceived cost of updates. The findings of our study support their second and fourth recommendations.

Security automation

Edwards *et al*. [20] argue that security automation strategies, removing the user from the decision process, may be more limited than anticipated. Framed across a spectrum of rigidity, as in Fig. 2, these strategies range from fixed, 'one-size-fits-all' policies to dynamic policies allowing users to personalize the process. The 'fixed policy' approach then represents the 'stupid user approach' [21], installing updates quickly and automatically without relying on the user. The outcome is a maximally secure system, albeit one where the system operates independently of the user's working context. We consider that the update model in Windows 10 Home Edition may sit towards this end of the spectrum.

Conversely, a 'dynamic policy' allows the user (rather than the software producer) to control the updating process; updates may not be applied as quickly, requiring an independent 'education approach' [21]. The update model in Windows 7 is perhaps analogous to this approach.

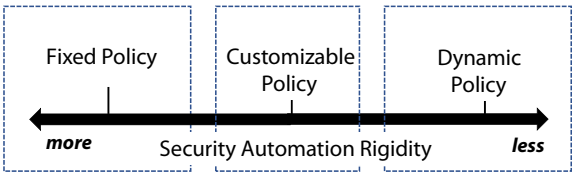

Figure 2: The spectrum of automation approaches, reproduced from Edwards, Poole and Stoll [20].

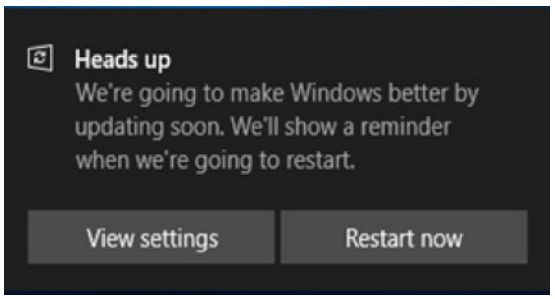

Figure 3: Initial notification of a pending update requiring a restart.

Windows 10 Home updates – feature analysis

Updates for Windows 10 Home Edition, released in July 2015, differ significantly from previous versions of Windows. First, updates can no longer be installed selectively. The update process is also arguably more imposing, with Home Edition users at one point no longer being able to disable automatic updates. Users will be informed of a need to restart their device to complete an update (see Fig. 3) and be reminded if they ignore this (see Fig. 4), allowing a user to choose a specific time for the restart.

In the absence of any intervention from the user, downloaded updates for previous Windows versions were installed during a dedicated maintenance cycle scheduled (by default) at 3 am. Windows 10 automatically installs updates immediately after download. As the default maintenance cycle was designed to never take machine resources away from an active user,[2] this represents a significant change in update behaviour for Windows 10, as resources (and potentially battery life) are consumed while the computer is in use.

Methodology

For lack of an existing description of the Windows 10 Home automated update, we built a model of its user-facing functionality. We adopted an approach similar to Wash *et al*.'s documentation of the Windows 7 update model [15]. We (i) compiled a list of features and functions described in release announcements and on the official Microsoft Community Support Forum, then (ii) verified them in an Oracle Virtual Box environment using a black box testing approach. The verification began by taking a virtual machine snapshot of a fresh, default installation of Windows 10 Home Edition. Once Microsoft had published subsequent updates, the snapshot was restored to allow the virtual machine to download them. Shortly before the download completed, a further snapshot was taken. By repeatedly restoring to the second snapshot, we were able to

2 Automatic Maintenance (Windows Dev Center), https://docs.microsoft.com/en-gb/windows/desktop/TaskSchd/task-maintenence.

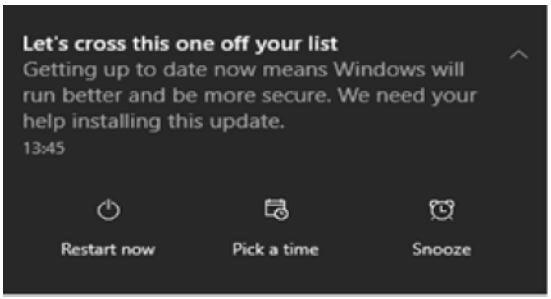

Figure 4: Example reminder notification of a pending update requiring a restart.

efficiently investigate the machine's behaviour as the update was applied with different control paths selected.

Due to the timing of the study, we focused on version '1803 – April 2018 Update'. The forced update model of the 'Home Edition' should then have meant that users regularly connected to the Internet would be running it. As the '1803' feature update occurred shortly after the start of our study, we were able to experiment with the installation of this feature update as well as quality updates.

The flow chart in Fig. 5 represents the update model of Windows 10 Home version 1803 built using our approach. The process of populating the model was informed by Virtual Machine (VM) experiments and a review of related literature, but not assumed to be exhaustively complete; the discussion that follows is informed by the model. The behaviour of the update mechanism is dependent on a complex range of user and system properties. Windows will check for updates daily, then download and install them without any further interaction or notification of the user.

Developing knowledge about update mechanisms

Figure 5 also illustrates the 'mechanisms' [22] involved in Windows 10 Home User Edition updates. Mechanisms are of interest in security and security-related user studies, towards developing knowledge about specific security-related features and the phenomena they produce. Visible phenomena are of interest in the study of software updates, as there are both 'silent' updates and forced restart updates. Also, updates may combine functional and security features in the same update, or be specifically for security reasons. The experiences a user has of the update will then be influenced by the behaviour of the update mechanisms. These are the 'entities and activities' represented by the various diamonds in Fig. 5 that produce visible phenomena that a user may see. They consist of visible prompts (denoted with 'Display' in Fig. 5) and hidden changes (e.g. feature changes) which the user is not directly prompted about, but which they may indirectly notice after the fact (e.g. if a menu arrangement or icons have changed). Studies such as [15] combine technical and user-centred analysis, which addresses both at the same time. Software functionality (including operating systems and their update features) may change over time, so being able to concretely define the features under observation is useful for sharing knowledge about how to improve a system towards improving its defence.

Mapping user interaction with updates

To install updates that require a restart, users must either restart their computer themselves or ensure that the computer is on or in sleep mode when the update is due to be installed. For the latter, this time will either be outside of the configured 'active hours', or at a specific restart time nominated by the user.

With Windows 10 Home Edition, there are now two separate control flows. In the first flow, either the user sets an explicit restart time within the following 7 days, or the restart occurs outside the specified 'active hours' when the computer is not in use. If the user has selected a specific time for the restart, a notification is displayed 15 minutes before the scheduled restart, at which point the user may select a new time or explicitly initiate a restart at that moment. If the chosen time of restart arrives, we have identified two alternative cases depending on the type of update being installed. If a quality update is being installed (i.e. a bug fix or security update), the computer is restarted at the chosen time regardless of user action. For other updates, if the computer is in use, the restart is automatically rescheduled to occur a short while later (between 30 and 60 minutes in our experiments).

It is useful to compare our flow chart to the flow chart documented for Windows 7 update functionality, as produced by Wash *et al.* [15]. In a similar fashion, we have identified key user decisions and actions. However, our flow chart shows that a user may be presented with a different message depending on how they have responded to notifications and decision prompts from the operating system (in our case, Windows 10). Wash *et al.* imply in their flow chart, for instance, that a user can repeatedly postpone updates; we see with our flow chart that instead of this, the choices that a user has to postpone an update in Windows 10 are limited depending upon the nature of the update.

The second control flow relies on the 'active hours' feature, intended to minimize disruptive impacts of restarts by preventing restarts during these hours. It is a machine-wide setting that was added in the '1607—Anniversary Update' (released in July 2016), allowing users to specify a time period of up to 12 h (and then later 18 h in the '1703—Creators Update', March 2017) during which a computer will never automatically restart to finish installing an update. If the setting does not align with a time when the computer is in use, a user who perhaps moves away from their computer outside these hours may return to find their machine having restarted, and any stateful tasks running at the time of the reboot (such as a series of large file downloads) disrupted by the restart. To prevent this, Microsoft provides developers with an 'Application Recovery and Restart' Application Programming Interface (API)[3] that applications would need to support to guarantee that their applications are seamlessly restored after a restart. Unfortunately, not many applications have implemented this feature, as we show below.

Prompts and reminders for updates

As a safeguard, Windows 10 displays a reminder notification 15 minutes before the restart time and checks for the computer being in use (see 'Computer in use' section) before restarting (the lower left- and right-hand side of Fig. 5). This helps to avoid restarting the computer if actual computer use does not adhere to the active hours configured for the machine. If the computer is in use, the user is offered the chance to select an explicit time for the restart, or to restart the computer at that moment. If the message is ignored, a new time outside active hours is imposed.

Similarly, if updates are downloaded outside of active hours, a user may return to their computer at the resumption of active hours to find it has restarted, with any in-progress tasks having been

3 "Registering for Application Restart (Windows)", https://docs.microsoft.com/en-gb/windows/desktop/Recovery/registering-for-application-restart

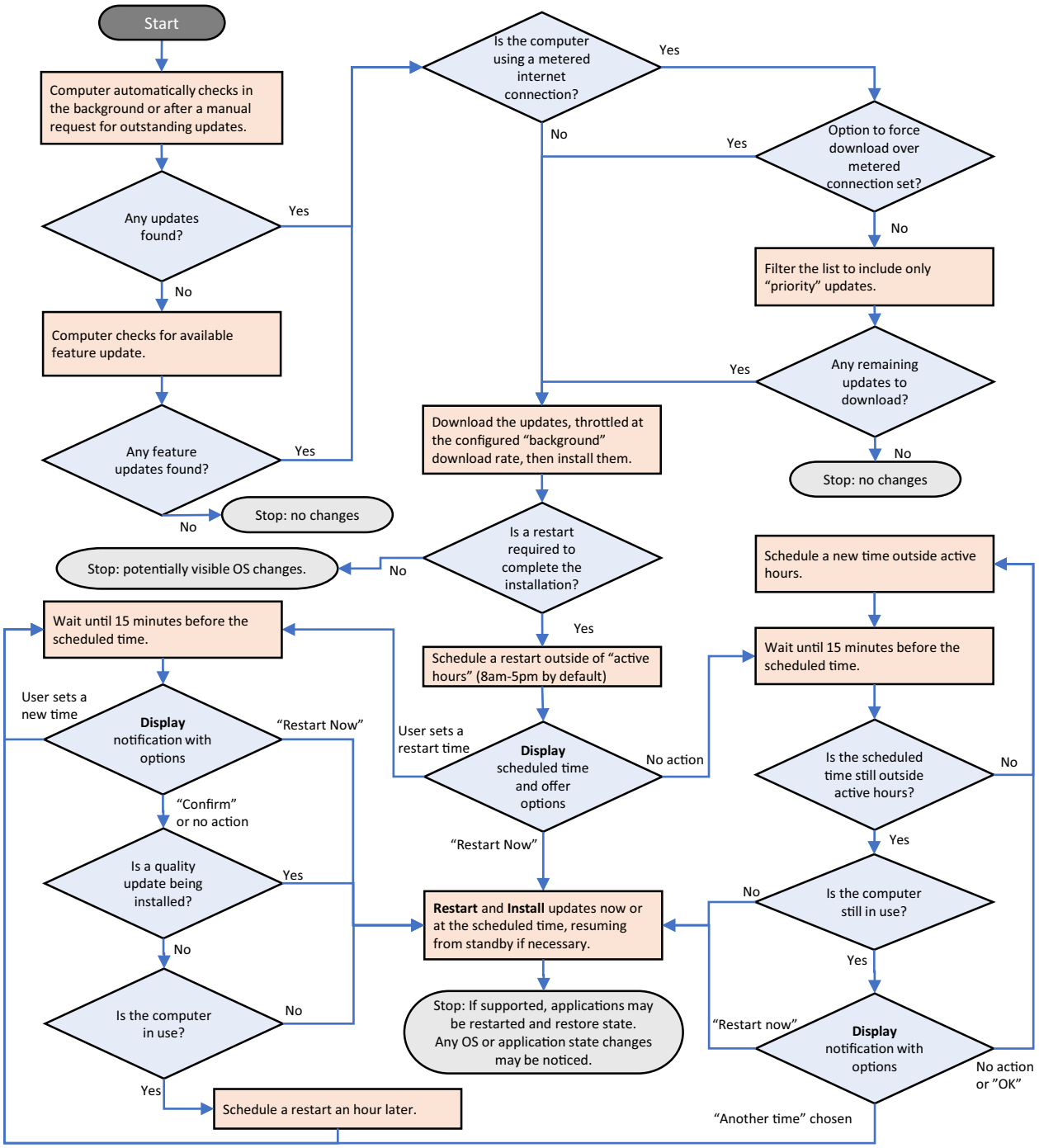

Figure 5: Windows 10 Update model. As the computer shuts down in preparation for installing an update that requires a restart, the message 'Configuring Windows Updates—Don't turn off your computer' is displayed. During the subsequent start-up, 'Working on updates. Don't turn off your PC. This will take a while.' is shown. Each stage has a separate progress bar; one during shutdown and one during the restart. If the 'Sign-in' option to 'reopen my apps after an update or restart' is set, Windows will attempt to restore the state of the user's desktop to the state it was in before the restart.

disrupted. Windows 10 does not provide a user interface for users to control when the background check for updates occurs.

From a security perspective, users need to understand the need to restart their computer to complete the installation of some updates. To minimize disruption, there is a burden on users to become skilful in using the 'active hours' feature (and its very concept), and conversely that active hours can be aligned with their usage patterns. Otherwise, a user cannot reliably leave applications running outside of 'active hours' or have an expectation that their desktop state will be fully restored after a restart. This constitutes a significant change from previous behaviour. These last two expectations are arguably unnatural, being counter-intuitive to the physical world: if we temporarily leave our possessions unattended but secure, we expect to return to find them how we left them.

Computer in use

Windows tries to determine if the computer is in use to avoid restarting it if it is. We used mouse movements and clicks in our virtual

environment to simulate the presence of a user in these experiments. We found that watching a video in full-screen mode did not register as user presence and the VM subsequently restarted. This is despite there being potentially numerous means by which Windows might detect user presence [23].

Survey methodology

In this section, we contrast the expectations of the Windows 10 Home update model to users' perceptions and reported experiences using the operating system. In particular, we focus on specific Research Themes:

- RT1: The need to restart a computer when updates are installed;
- RT2: The need for restart to be approved by users;
- RT3: The need to reopen applications before being able to resume work after a restart.

We designed an online survey to capture user experience with the above. The survey was prefaced with questions about general computer use, such as when the computer is used, whether it is shared with others and if the participant is wholly responsible for 'looking after' the device. This informed the visibility participants had of operating system prompts.

Subsequent sections of the survey then captured existing knowledge of what operating system updates do, perception of the risks that security updates are intended to address and how participants interact with updates and update (prompts) (such as identifying the conditions under which an update may be postponed, and how). Proactive security behaviours were also explored in the survey, alongside questions to determine if participants were aware of features for tailoring the update process, such as configuring the 'active hours'. The full survey instrument and survey results file are available (see 'Data availability' section and Appendix). The survey design was informed by our model (as illustrated in Fig. 5). The study was approved by our department's ethics review process.

Survey design

The VM analysis in the previous section (and illustrated in Fig. 5) provides a foundation for understanding the context of Windows updates from the view of the user. This is critical for developing an understanding of the feature mechanisms which influence user experience of software updates, depending upon how they respond to user activities. As in Fig. 5, there are specific points in the update process where a user will be presented with a notification (where the operating system will 'Display' a prompt, such as options for how to install a pending update), or experience a particular 'Stop' state (including that the appearance and function of the operating system have changed in some potentially noticeable way). We capture context of use (Q5–Q15, as in Appendix); factors relating to willingness to respond to update prompts (Q16–Q18); participant responses to prompts such as those which Windows Home Edition may 'Display' to a user (Q19–Q32); any proactive behaviours which participants engage in which relate to how the update mechanisms will behave (Q33–Q42); and participant perceptions of other stakeholders in the software ecosystem and their own capacity to recollect how their computer software is behaving and has affected them (Q43–Q44).

Recruitment

The survey was open to residents of the UK aged over 18 years, who had completed at least five prior studies on the dedicated Prolific survey platform and who had an approval rating in excess of 90%. We requested an additional participant filtering criterion on Prolific for the operating system on a participant's primary computer. At the time of data collection, 1862 potential participants claimed to use Windows 10 Home Edition, 419 Windows 10 Pro Edition, 42 Windows 10 other editions. Totally, 621 participants stated that they were using Windows 10, but were unsure of the edition; 479 participants used other Windows versions. We required our participants to be users of 'Windows 10 Home Edition' on their primary computer. Participants were compensated £2 for completing the survey. Although we had 98 responses, one participant failed one of two attention questions and was removed from the results. We chose to exclude a further four participants who reported high uncertainty in the answers they provided in a dedicated closing question. This gave a final count of 93 participants.

Demographics

The demographics of our participants can be found in Table 1. Compared to the general public, our participants are more likely to be students (14% vs. 3% in the wider UK population). Many previous studies about software updating [3, 15, 17] have also drawn participants from academically biased pools. These participants might be more technically savvy, with more technically accurate mental models of updates. However, we only observed minor differences in the responses for participants who had ever worked or studied in a computer-related field, which do not influence our conclusions. This is in line with findings from Forget *et al.*, whose participants with greater engagement in computer security and maintenance did not necessarily have more secure computer states [24]; however, Ion *et al.* note that computer experts mention system updates 30% more frequently in their top three pieces of security advice than non-experts [5]. We also asked the age of participants' computers, to serve as an approximate indication of how many monthly update cycles and 6-monthly feature updates they may have experienced. This also acted as a general indicator of how much of an impact updates might be having on their system's performance.

Survey results

A third (31) of our participants reported having worked or studied for a qualification in a computer-related field. Totally, 96% (89) participants reported extensive or moderate experience of at least one version of Windows prior to version 10; 82% (76) described their own experience with Windows 10 as extensive and a further 15% (14) as moderate. Two-thirds (64) were the sole, regular user of their computer. Many of the remaining participants (26) reported sharing their computer only with other people in their household. Totally, 90% reported doing all (48) or most (36) of the maintenance of their computer themselves. Regarding how often participants used their computer, 90% reported using their computer on at least five days each week. With respect to the participant's computer itself, around two-thirds (64) were laptop devices and 26 were desktop computers. Totally, 81% (75) described the speed of their computer as either 'fast' or 'neither noticeably fast nor noticeably slow' in almost equal numbers. None of the participants described their computer as 'very slow'. The median reported age of computers was between 1 and 2 years. We then consider that computer performance would not directly exacerbate reported experience of updates (rather than an ageing computer being the fundamental cause of any bad experiences with the operating system).

Table 1: Demographics of the user study

Age groups (years)		Age of computer	
18–24	14	Less than 1 month	2
25–34	32	Between a month and 6 months	7
35–44	18	6–12 months	9
45–54	16	1–2 years	33
55–64	11	2–3 years	14
65–74	2	More than 3 years	28
Gender		Student status	
Female	58	Student	13
Male	35	Non-student	80
Education		Employment	
No formal qualifications	1	Unemployed (and job seeking)	10
Secondary school/GCSE	9	Not in paid work (e.g. homemaker, retired)	16
College/A levels	28	Part-time	23
Undergraduate degree	42	Full-time	41
Graduate degree	11	Other	3
Doctorate degree	2		

When computers were not in use, just over half (49) of the participants reported regularly 'shutting down' their computer. Most of the remainder (39) reported that their computer was left switched on. Whether the computer subsequently entered sleep mode was not important to us because in both cases, by default, the computer would be woken to complete the installation of an update.

With respect to the activities for which participants used their computers, all reported browsing the Internet and most reported using office productivity applications and social media. The two categories of uses with the lowest levels reported were for playing games and video calling, with each reported by approximately half of participants.

Perception of activities related to updates

While participants agreed that updates helped to keep them safe, there was less clarity about what updates did. Of the participants, 29% either did not know, or believed that updates rarely or never fixed errors in software. In contrast, 87% thought that updates add new features at least occasionally, implying our participants thought software updates add features more frequently than they fix errors. Interestingly, Redmiles *et al.* [25] similarly found that 40% of their participants perceived that software updates occurred to fix errors and prevent crashes.

Our participants on average perceived updates to be published less frequently than Microsoft's monthly release cycle. Those with a computing background were about 3 times less likely to say they did not know the update cycle (2 out of 31) than those without (11 out of 62), but their answers were not statistically significantly different. Of those who gave an answer, 49% (39) thought that new updates were published approximately every 2 months or less frequently. This was despite an incorrect belief held by half of all participants (47) that they always needed to restart their computer when updates are installed. This needs to be considered in the light that monthly cumulative updates are a subset of all updates and always require a restart. Even if we restricted our analysis to participants who are sole users of their computer (and thus might reasonably be expected to be aware of all activity on it), and who believe updates always require a restart (35), the prevalence of the belief about the incorrectly low frequency of updates was still evident (18).

When asked about the frequency with which updates are installed automatically, only 17% (16) of our participants chose 'Always'; 42% (39) selected 'Often'. Aside from 5% who stated that they did not know, almost all participants believed they are never charged for updates.

Use of dedicated Windows 10 update controls

As we wanted to assess how well the Windows 10 update model fitted the needs of users, it was essential to understand how participants used their computer beyond their interactions with updates. Given the key role the 'active hours' feature plays in managing the disruptive impact of updates, we assessed whether participants' reported patterns of use aligned with its assumptions, mainly that for 'active hours' there is a period of at least 6 h each day when the computer is switched on (or on standby), but is not in use.

We asked 'What happens to your computer when no one is using it?' and provided a range of different options, some of which were equivalent from an updating perspective, such as 'It is left on all the time' and 'It is put into sleep mode'. This was to reduce the need for participants to convey their interactions with specific interface features and computer functionality. We then asked how many days in an average week the computer was used, and what the typical hours of use on weekdays and weekends were. Given that 'Patch Tuesday' occurs on a weekday, the former was particularly important. We separated the day into 3-h intervals, specifically aligned with the default value for 'active hours', namely 8 am to 5 pm. We hypothesized that this might be a poor choice of default for discernible groups of home users (such as those with '9 to 5' jobs, or those in study). As the feature is not referred to during the initial set up of Windows, we also hypothesized users may be simply unaware of its existence. Consequently, we also asked if participants were aware of the feature, and if they were, whether they had configured it. By asking users how often they used their computer, we had hoped to revisit Furnell *et al.*'s hypothesis [26] that infrequent users had more negative perceptions of updates than frequent users, however, only five participants reported using their computer for less than 5 days a week.

We made two key findings relating the 'active hours' feature. First, only 28% of our participants were aware of the existence of the active hours feature. Those with a computing background were significantly more likely to be aware of it (15 out of 31) than those without (13 out of 62) [$X^2(1, N = 93) = 6.83$, $P = 0.009$]. Secondly, most of the usage patterns reported among our participants do not fall within the default time window of 8 am to 5 pm (see Fig. 6). All but six of our participants reported typically using their computer

on weekday evenings. The hours of use of just three participants fell within these limits, all of whom were sole users of their devices. Looking at whether 'active hours' could be set to align with participants' reported usage, 50 of the 64 'sole computer user' participants had an unbroken 6-h interval of non-use (as required for the feature to function best).

We also asked participants who were aware of the feature whether they had changed it from its default setting. Of the 26 participants that were aware of the feature, 10 had not changed it from the default despite their reported usage patterns being incompatible with the defaults (Fig. 6). We hypothesize that the users were not aware of this mismatch themselves (being prompted in the survey may have been a first chance to reflect upon this, for instance).

We tested the answers given by those aware of the 'active hours' feature against related questions for signs of significantly different experiences, e.g. whether they had experienced an unexpected restart, or whether they felt the computer always sought their permission before restarting. None of these tests showed statistically significant variations.

Proactive check of updates

Half (46) of the participants reported having proactively checked for updates in the past. There was no statistically significant correlation with the participants' computing background. As to the reasons why participants checked for updates (Fig. 7), the most popular reason overall, and particularly among participants who chose exactly one of our seven possible answer options, was to fix non-security, technical problems. The second and third most popular choices were to check that updates are working and to better control when updates are installed. Being more perceptive to security risks was not a predictor of participants' inclination to check for updates, and checking for updates to fix security problems was only our sixth most reported reason. It was selected by none of the 25 participants who chose exactly one reason.

Users can limit the installation of updates by marking a network connection as 'metered'. Only six of our participants reported having employed this workaround. Although some online forums we had encountered had suggested this technique was particularly prevalent among gamers, they only accounted for half of the six, approximately the same proportion as across the survey sample (including those who did not declare an interest in games).

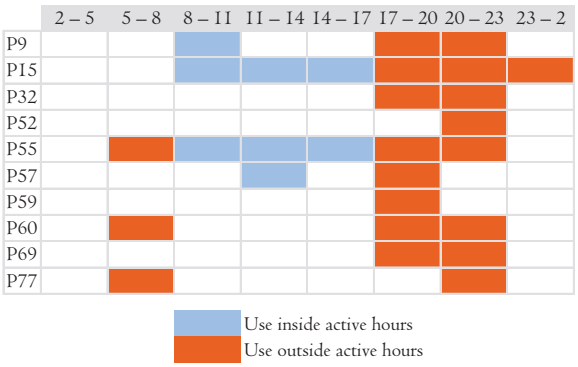

Figure 6: Usage pattern of participants who reported being aware of 'active hours', but are using the default settings despite these being incompatible with their usage behaviours.

Handling restarts

Due to the potential for restart requests to be particularly disruptive, we specifically wanted to capture how home users handled them. We wanted to understand what choices participants made and whether the features designed to help minimize their disruption were being used. We did this by constructing two hypothetical update scenarios within our survey (see Q19 and Q24 in Appendix). The first concerned the installation of a monthly cumulative update requiring a restart. The second, the installation of a feature update. To aid participants' recall, we illustrated our questions with screen images showing notifications for the restart scenarios (sampled from our virtual environment). The images reflected an 'out-of-the-box' Windows 10 desktop with no personalization. The answer options were intended to elicit how a participant planned to eventually comply with the request for an (inevitable) restart. For both, we asked participants to imagine they were in the middle of an hour-long task on their computer that was important to them when the request appeared. If they chose to 'Restart now', we interpreted that choice as the most disruptive option given the context of the question. Ignoring the notification is potentially the least disruptive option, however, if the user forgets about the pending restart but leaves their computer switched on but idle, the computer will restart itself, then possibly resulting in the loss of unsaved work.

We followed each scenario with a question to ask about participants' expectations for how long each restart would take, as a high-level analysis of customer support forums suggested users felt it was too long. Indeed, this has been an area of recent focus for Microsoft [27]. Around 7% of participants reported that they would 'Restart

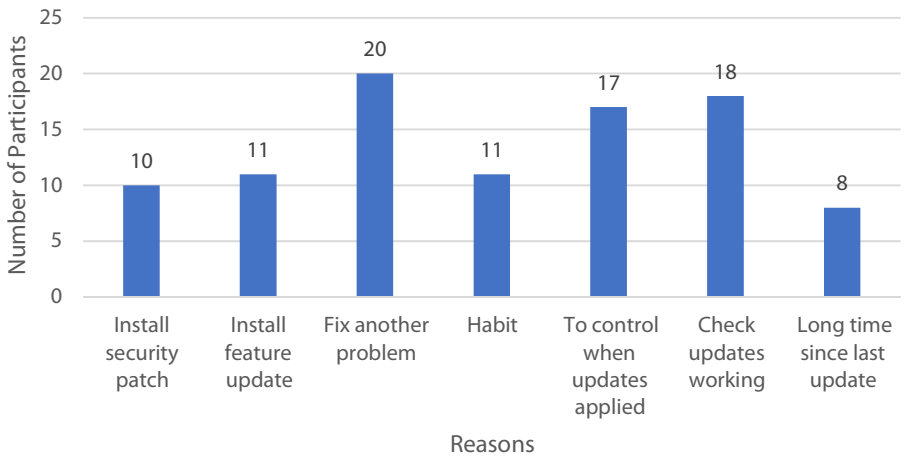

Figure 7: Reasons why participants proactively checked for updates. Participants were able to select multiple reasons.

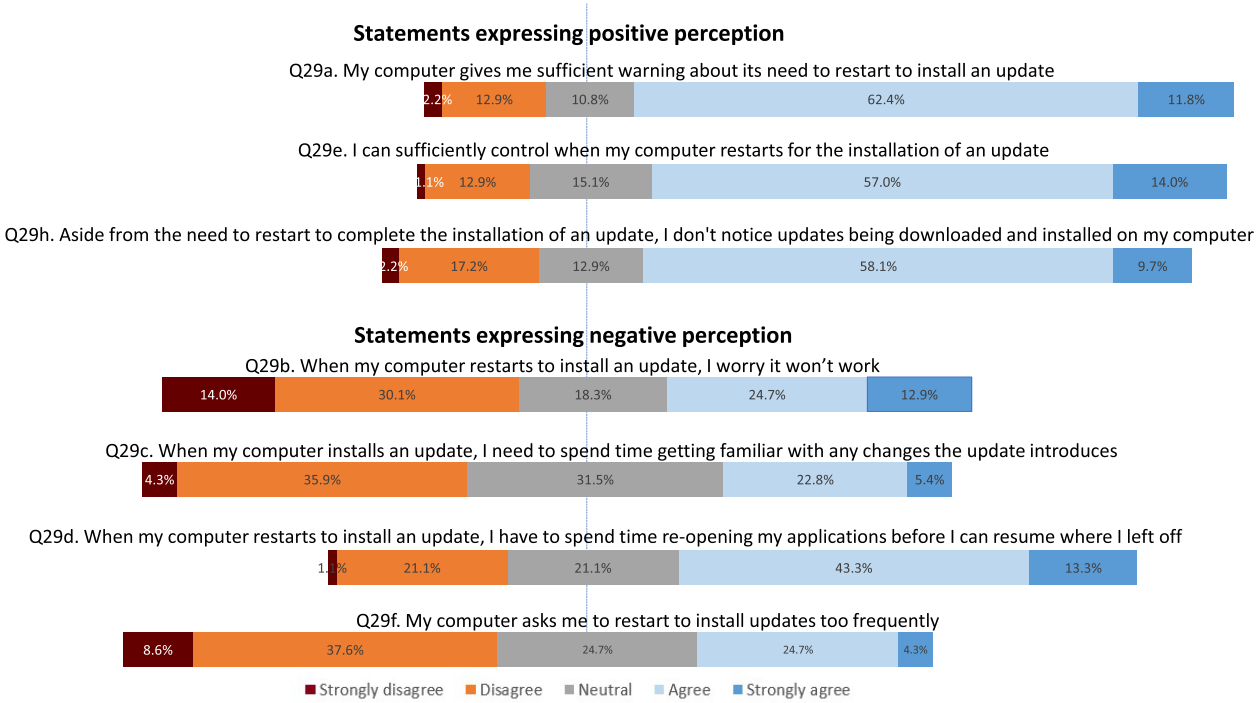

Figure 8: Participants' perception statements relating to updates.

now' for both scenarios. In the first scenario, 30% (28) chose to restart the computer themselves once their task was complete; 40% (37) chose to 'update and shutdown' after they had finished using their computer; 30% of this latter group had previously stated that their computer was left on when not in use. When users were nudged towards picking a restart time in our second scenario, 40% (37) said they would choose this option, however, 53% said they would choose to be reminded later with the intention of taking control of the restart themselves (regardless of having chosen a restart time).

With respect to the expected duration of the restart, approximately half (45) of our participants gave identical estimates for both scenarios; 58% of those (26 of 45) expected both restarts to take less than 15 minutes, and only two participants expected to wait for more than 45 minutes. Two participants gave a lower estimate for the 'longer' feature update.

Sentiment towards updates

Our participants were generally positive towards updates overall. Referring to Fig. 8, participants generally expressed positive sentiments about being given sufficient warning of pending restarts to apply an update; about controlling restarts and; not noticing updates downloading and installing in the background. On our two questions about a worry that the computer will not work after an update and there being too many restarts, desktop users were more complimentary than laptop users, but the result was outside statistical significance. A summary of our results of Likert scale questions of participants' past experiences with updates can be seen in Fig. 8.

Our survey had two sets of comparative questions. The first asked participants with experience of prior versions of Windows to indicate whether they felt updating Windows 10 was first easier and secondly causes fewer interruptions. On the former, 53% agreed and only 8% disagreed. On the latter, 43% agreed and 21% disagreed. The second comparative question asked participants to compare their trust in Microsoft's ability to provide updates with other software producers. Of the participants, 95% perceived Microsoft to be better (33%) or as good as (61%) other software producers.

Perception of online risks

We wanted to understand participants' perception of the computer security risks which updates protect them from. We asked a Likert scale question to assess if participants thought cybercriminals target 'other people' [28], whether they thought their machine could be used to facilitate crime (e.g. as part of a distributed denial-of-service attack), and whether participants related their personal security to the security of the websites they trust.

The majority of participants agreed with all our positively worded, Likert scale items about the information security risks mitigated by updates. Levels of disagreement ranged from 24% to 4%. Most users considered themselves not to be worthwhile targets, consistent with Wash's 'Big Fish' model [28]. These responses did not predict statistically significantly knowledge of the existence of the active hours feature. We did not find any sub-groups with statistically significantly different answers.

Impact of updates on other tasks

Just under half (44) of our participants reported experience of their computer restarting unexpectedly to install an update. These same participants were significantly (Fisher's exact test $P < 0.05$) more likely to agree with our statement that there were too many restarts to install updates, to disagree with our statement that they had sufficient control over when their computer restarted, and to disagree with our statement that their computer gives them sufficient warning when it needs to restart.

While a majority – 57% (52) of participants – said the duration of restarts met their expectations, 42% (39) said they took longer

than expected. This is similar but slightly more positive than Vaniea and Rashidi's finding [29] for their users' perception of update installation times (at 43% and 45%, respectively). Only one participant did not express an opinion. In a related question, half of participants agreed that the longer a restart took, the more concerned they became, and 70% of participants were positive about the helpfulness of the notifications in providing progress information during a restart. This latter result appeared to contradict the work of Vitale *et al.* [30], however, they appear to have considered updates to Windows 10 from a previous version number. An aspect of restarting a computer that our participants generally agreed with overall was the need to spend time reopening applications after a restart before primary tasks could be resumed (57% agreed, while 22% disagreed, see Fig. 8).

Application restart – analysis

Users may avoid software updates which interrupt their tasks, but may also avoid updates which are presumed to require not only a context switch away from their tasks, but also a need to restart the applications they were working with [31]. Where prior studies have considered how best to situate updates in users' lives, with this part of our study, we consider one way to directly reduce the costs of updates which interrupt the user: the capacity for applications to restore their state prior to a restart (informing RT3). Windows 10 offers such functionality.

Analysis methodology

As mentioned previously, Microsoft provides developers with an 'Application Recovery and Restart' API [32], which applications would need to support to facilitate the full recovery of a user's original session after a restart. This API allows Windows to tell running applications that a restart is inevitable, prompting the application to save its current state and request to be restarted once Windows has resumed. This requires applications to support a comprehensive save and resume feature, where not just unsaved work is preserved, but also potentially long-running processes can be paused, saved to disk and resumed at a later stage.

If all applications supported this API and implemented comprehensive features for saving and restoring sessions, an application could be suspended and resumed by the operating system without any loss in state and without affecting user's activities (other than the delay induced by the system restart). This architecture would be akin to the behaviour of the Android operating system, where this pause, save and resume design is ingrained in all applications [33]. This design choice can be attributed to constraints on the memory and processing power of mobile devices, but nevertheless illustrates an architectural design where applications do not assume uninterrupted access to resources.

In this section, we measure the spread of adoption of the 'Application Recovery and Restart' API, and to what extent applications support it. We first introduce the sources of the applications we study, then we describe the experimental setup of this study and we subsequently discuss the findings.

Application selection

We selected a broad variety of software applications representative of those frequently used by both home users and businesses. We identified several websites that recommend 'top' applications for specific uses (namely TechRadar, Lifehacker, MakeUseOf) and two lists of most popular software (by Microsoft and Amazon). We also assessed a selection of software from our institutional software repository, as it offered a wide selection of paid-for software. This method of sampling is inherently based on convenience, where we acted to cover a broad range of software applications that are in common use. The full list of applications and the exact software version used can be found in Table 2.

All applications are actively maintained (including recent version increments). We are using the latest versions available at the time of study, in May 2020. The data collection was carried out once before, in June 2019 (although MS Teams, Zoom and Discord were only tested in May 2020), with the most recent versions of the software at that time. No changes in the application behaviour were noticed between the two points of data collection. Given that Windows 10 was first released over 4 years ago, we argue that there has been sufficient time for application developers to implement the API in their software.

Experimental setup

We created a fresh installation of Windows 1809 with no further patches in a Virtual Machine. The choice of version of Windows is not essential for this section as we are studying application behaviour and not Operating System behaviour. The aforementioned 'Application Recovery and Restart' API has been unchanged since the first release of Windows 10 [32]. All applications were installed on the VM. In order to elicit a realistic response from the application to a restart triggered by a Windows update restart, we chose a state for each application which we deemed likely for the application to be left in by users; e.g. having multiple tabs open in a Browser with some unsubmitted form data entered into a tab; or having navigated to a specific path inside a compressed file. Once the application was put into an interim state, we used the 'Pick a time' functionality from Windows Update as shown in Fig. 4 to set a time more than 15 minutes in the future, and left the VM unattended (i.e. no further mouse or keyboard interactions). At the specified time, Windows closes the running applications, installs updates and restarts. Upon restart of Windows, we inspect the state of the applications. Due to memory limitations, we batched subsets of running applications into groups for the experiment (not all applications were tested together in the same instance). We used the VM's snapshot tool to achieve identical system setups and repeated each experiment twice, observing identical results.

Findings

Our full experimental results can be found in Table 2. Of the 47 applications studied, only 9 restarted automatically after Windows rebooted. These were mainly browsers (Chrome, Firefox and Internet Explorer, but not Edge) and communication tools (MS Teams and Discord, but not Zoom), as well as MS Word, Endnote, Spotify and Sibelius. Of these nine, MS Word and Sibelius both displayed a user prompt for a data recovery mechanism, rather than immediately resuming the previous session.

Only Discord and arguably MS Teams restarted and fully restored their previous state automatically (according to our criteria). Whether MS Teams should rejoin an active call automatically without explicit user interaction can be argued: it is used mostly in a professional setting with video enabled. MS Word and Sibelius also came close but the user interface layout was lost and additional user interaction was required to resume work.

There are a further 14 applications that were not restarted automatically by Windows, but which do make a reasonable attempt at

Table 2: Behaviour of commonly used software when Windows initiates a restart to install updates

Name	Version	Experimental setup state	Automatic restart	State recovered	Unsaved data recovered
7-Zip	19.00	Zip file opened in UI	×	×	
Adobe Acrobat Reader	2020.006.20042	Open PDF with unsaved comments	×	✓	✓[a]
Adobe Photoshop Express	3.0.316.0	Open picture with unsaved edits	×	×	×
Audacity	2.3.3	Open music file with unsaved edits	×	✓	✓[a]
Chrome	81.0.4044.138	Open two tabs with not submitted form data	✓	✓	×
Eclipse IDE	2020-03 R	Open multiple files with unsaved content	×	✓	×
Endnote	X9.3.3	Editing a reference	✓	×	×
Evernote	6.24.2.8919	Editing a new note	×	✓	✓
FileZilla	3.48.0	Quick connect to an SFTP server, 'remember passwords' not enabled	×	×	
Firefox	76.0.1	Open two tabs with not submitted form data	✓	✓	×
foobar2000	1.5.3	Play tracks from library	×	×	
Franz	5.5.0	Connected to slack, draft message	×[b]	✓	✓
Gimp	2.10.18	New unsaved image	×	×	×
IntelliJ	2020.1.1	Unsaved changes to a scratchpad	×	✓	✓
IrfanView	4.54	Image opened and zoomed into	×	×	
iTunes		Music playing from local folder	×	×	
KeePass	2.45	Adding new entry form	×	×	×
LibreOffice Writer	6.4.3	Unsaved document with content	×	✓	✓[a]
Mathematica	12.0.0	Unsaved document with content	×	×	×
Matlab	R2020a	Unsaved script with content	×	×	×
Mendeley	1.19.4	Editing notes of a document	×	×	✓
MS Office Word	1808 Build 10359.20023	New unsaved document	✓	✓	✓[a]
Notepad++	7.8.6	Open two new files with unsaved content	×	✓	✓
Paint.NET	4.2.10	New unsaved drawing	×	×	×
PeaZip	7.2.2	Zip file opened in UI	×	×	
RStudio	1.2.5042	Unsaved script with content	×	✓	✓
Shotcut	20.04.12	Edits to existing project	×	✓	✓[a]
Sibelius	2020.3	New unsaved score	✓	✓	✓[a]
Slack	4.5.1	Draft message	×[b]	✓	✓
Spotify Music	1.132.618.0	Playing a playlist	✓[b]	○[c]	
SPSS	26	Unsaved dataset	×	×	×
Sumatra PDF	3.2	Opened a PDF on Page 2	×	×	
Thunderbird	68.8	Draft an e-mail	×	✓	✓[a]
VLC	3.0.10	Playing a playlist	×	×	
WhatsApp Desktop	2.2019.8.0	Draft message	×	×	×
Zotero	5.0.87	Edit title of an entry	×	×	×
MS Teams	1.3.0.12058	In Teams call, messages typed but not sent	✓	✓[d]	✓
Zoom	5.0.2 (24046.0510)	In Zoom call, message typed in chat but not send	×	×	×
Discord	Stable 60315	In Discord voice channel, message typed	✓	✓[d]	✓
cmd.exe	10.0.17763.1	Existing history and command drafted	×	×	×
Internet Explorer	11.1.17763.0	Two tabs open, unsaved form data	✓	✓	×
Microsoft Edge	44.17763.1.0	Two tabs open, unsaved form data	×	✓	×
Notepad	10.0.17763.1	Unsaved file	×	×	×
Paint 3D	5.1904.8017.0	Unsaved drawing	×	×	✓[a]
PowerShell	10.0.17763.1	Existing history and command drafted	×	×	×
Remote Desktop	10.0.17763	Connection setup	×	×	×
Windows Explorer	10.0.17763.1	Multiple windows open, search open, edit file properties	×	×	×

Notes: To enable restarts that fully recover state, applications within Windows 10 Home Edition should automatically restart after windows updates have been installed, then recover the User Interface (UI) state and any previously unsaved data. We distinguish between the recovery of the UI state and the recovery of unsaved data, as there are some applications that do one but not the other. No tick or cross indicates that our setup did not test this feature.

[a]Marks where the application appears to use an integrated recovery mechanism, rather than explicitly saving state and data on shutdown.

[b]Marks where an application has autostart enabled by default.

[c]For Spotify, the playlist, current song being played, and position in the song are restored, but playback is paused and the home screen is displayed.

[d]For MS teams, the message conversation of the call was rejoined, but not the voice call itself, while discord automatically rejoined the voice channel.

restoring their previous state upon manual start-up. It would seem that these applications rely on their autosave features to minimize user inconvenience due to application crashes, and that restarts due to Windows updates are treated as application crashes. These are recoveries which are visible to a user, and not coordinated by the Windows restart API.

Individuals will need to spend time reopening applications, and while applications may recover some state (such as the contents of a

file), they may not recover the current activity within the application. For example in Table 2, applications such as Spotify came close to restoring the application session to exactly where a user left it. There are then potential subtle differences which may disorientate or delay a user, while they act to get back to where they thought they were in their use of an application.

Discussion

The silent success story

Informing RT1 ('Survey methodology' section), our participants perceived that updates added new features more often than fixing errors. Given that feature, updates occur approximately every 6 months and quality updates occur monthly, perception does not match reality. One possible explanation is that users do not notice changes after quality updates, but at the same time do notice them after feature updates. This may be a natural consequence of Microsoft's adoption of practices similar to Vaniea's recommendation [3], to disentangle updates that change the user interface from those that address quality issues.

Contrary to the study by Mathur *et al.*, our participants perceive updates significantly more positively [7], with updates not being perceived as disruptive or time-consuming. On Android, Marthur and Chetty report significant dissatisfaction with automatic application updates on Android [18], and 33% of their participants reported avoiding auto-updating their apps. However, their survey focused on whether a user had negative experiences. Given the high frequency of app updates on Android, it is likely that users are not aware of many updates happening. Here, a similar silent success story could also be present, and perhaps Android app updates should also become non-avoidable.

Regarding RT2, participants also underestimated the frequency of updates, believing that they occur less frequently than Microsoft's minimum release cycle. It suggests that some updates, including those requiring a restart, are being applied so silently [9] as not to be noticeable or memorable to our participants. The only evidence of a restart is closed applications, which were not restarted automatically after the reboot. It is perhaps then worth considering that when users are asked for their opinions of updates, what is reported may only refer to a subset of updates (specifically those involving a prompt, and requiring a restart, or those that change the user interface). Indeed, if applications can be fully resumed after a restart without any further user interaction, then opinions on updates may shift again. This is likely even more true on mobile operating systems, where apps are inherently designed to be stopped, and restarted by the operating system dynamically.

Future studies may need to combine system-level and user-centred study approaches. Where Wash *et al.* [15] differentiate between proactive and automatic updates, future system-level analysis may be useful for building a complete picture of what happens silently and what happens with the user's involvement. Revisiting the phenomena produced by an update, the study of updates is then a potentially decoupled system of update behaviours (be they visible or not) and update consequences: a silent update could produce changes which a user may or may not notice (as in the various 'Stop' conditions noted in Fig. 5, notably when an update is installed but does not require a restart).

4 Given our minimally specified virtual environment, our measurement may be close to the worse case.

Keeping the appreciative user adequately informed

Addressing RT3, participants did not appear to recognize and appreciate the implications of different types of updates (monthly cumulative vs. feature). The cues used by Windows are subtle, but the implications are potentially significant. As part of our own research, we measured the time taken by a cumulative monthly update in our virtual environment. Where this took 12 minutes, the feature update took 12 times longer.[4] Microsoft claims that the average time for the April 2017 feature release was 82 minutes [27]. Therefore, we think a notification that describes an update as one 'that could take a little longer than other updates' is failing to set accurate expectations to support users in planning around the impact of updates upon system availability. This may be supported by our general finding that participants believe restarts take longer than expected. Currently, Windows gives neither an estimate before nor during the updating process, and our own research showed the progress indicator can progress unevenly. Vitale *et al.* [30] made similar observations, enforcing the findings of Vaniea and Rashidi [29]. They argue 'reasonable [time] estimates must be possible', which we agree with.

Designing for consistent update behaviours

Based on our analysis of Windows' update model, we believe that Windows is not sufficiently explicit in seeking user permission for updates and restarts. It has been designed to nudge users towards updating as quickly as possible. It may give users the impression of having a greater degree of control over restarts than they actually do. Although the initial restart notification offers a 'Restart now' option, the implied and less explicit alternative is to restart later at a time of the computer's choosing, outside of active hours. However, from our survey, we have learned that this feature is unfit for its use. It then becomes the responsibility of the user to intervene should they wish to stop it. Unlike other consumer-focused operating systems that provide a visual reminder of a pending restart [34], Windows 10 Home Edition does not. Our finding may be explained by the notion that experiencing an unexpected restart may make users more aware about their lack of control. One might think that negative experiences here do not matter, as the user is unable to do anything about updates of Windows, however, these negative experiences can lead to users disabling updates on other systems too [18].

An existing control that could remedy this is to pick an alternative time within the next 7 days for the restart. Unlike restart times chosen by the computer, the computer may restart at this time even if in active use. This is a potential source of confusion given the promise to 'show a reminder when we're going to restart'. If a user is absorbed by other tasks then the computer could, in the mind of the user, appear to restart unexpectedly despite them having been responsible for the chosen time. Based on the findings here and in existing literature, we advocate that one's computer should not reboot while in active use.

The 'update pending' notification in Microsoft Windows nudges users towards restarting their computer immediately, with no second chance to postpone a restart if they choose 'Restart Now'. While we did not specifically ask whether this could have been the cause of any unexpected restarts reported by our participants, it is of note that only six participants in our first scenario and seven participants in the second scenario chose the 'Restart Now' option. Constantine and Lockwood's [35] 'Simplicity Principle' of user interface design recommends making common

tasks short and simple. Our data suggest 'Restart Now' is not a common choice, putting into question whether it is an appropriate option to display.

Perceived value of operating system updates

Further informing RT1, participants conveyed a perception of value in updates. Updates are being applied, and at the same time are not perceived to cause much (if any) disruption. However, the 'shock' of updates that create problems is not avoided, an example being the initial release of the '1809' (September 2019) feature update; installation of update 1809 deleted the personal files of a very small number of users with a particular configuration [36]. The update was subsequently withdrawn. Relating this to RT3, to adopt an update model like that of Windows 10 Home Edition is to shift some of the burden of effective updates onto developers. This is to ensure that updates are not 'destructive', especially if the user has no choice as to whether to avoid the update or not. Given our measurements in 'Application restart – analysis' section, it appears that application developers have not adopted this responsibility as envisaged. While Windows offers the ability to uninstall updates, this would not recover lost user data in the above example. If there is not a guarantee that updates can avoid being 'destructive', perhaps Windows ought to integrate an automatic snapshot feature that allows for immediate roll-back.

Limitations

The survey study suffers from similar limitations to other survey studies in security, namely that behaviours are self-reported [37]. One further limitation is that we were unable to query participant's experiences immediately after the update events. Some of the reported information, such as perceived event frequencies and impacts, may be informed by experiences distant in time. However, these are nonetheless the perceptions held by participants who are active users of Windows 10 Home Edition. If users were given more capacity to shape the (albeit increasingly unavoidable) update process, their perceptions of past experiences may govern how they configure future interactions with update mechanisms.

Even though half of our participants reported that their machine had restarted to install an update unexpectedly, we did not explore the consequences (such as data and state loss) they experienced. However, given our analysis of applications supporting the restart API, we suspect that participants were likely to have spent a notable amount of time on recovering from these unexpected restarts.

Conclusions

Here we analysed the behaviour of the automatic update feature of Windows 10 Home Edition, contrasting behaviour with an online survey of the experiences and perceptions of 93 UK-based users. A model of Windows 10 Home Edition behaviours highlighted inconsistencies in the restart behaviour. In one set of circumstances, Windows would reboot to finish installing quality updates even if the device was in active use. The default setting of the 'active hours' feature was compatible with the usage pattern of only three survey participants. Only 28% of participants were aware of the active hours feature. If properly adjusted, the usage pattern of 78% of participants could be captured by the active hours feature. It is not surprising then that around half of participants reported experiencing unexpected restarts.

Despite this, the automatic update behaviour of Windows 10 can be considered a (perceived) success. Our participants valued the updates and trust in Microsoft's ability to provide updates that benefit them. The quality of updates and the delivery of updates appear to be sufficiently reliable that our participants did not report an impact from quality updates.

Applications can do a lot more to reduce the impact of an unexpected restart. It appears that Windows applications continue the 'always on' and 'always available' view of devices and their resources. Windows restarts are not incorporated into the application's lifecycle design. The current approach of Windows' restart API is modest, yet none of the applications we studied has fully implemented the approach.

Recommendations

While it is important that security updates are installed in a timely manner, we believe that Windows' current policy is overly static. Given that many applications do not yet support Microsoft's restart API, restarts should only occur automatically if all running applications support this API. It is not obvious to users if an application supports this feature, where Microsoft could use its market position to improve support. Regardless, we believe that restarts should not occur if the system is in active use (especially so if retrieval of application state is not guaranteed).

The 'active hours' feature is arguably flawed. Prompts to users act to shape the installation of updates, but not the shaping of preemptive controls such as active hours: relating adaptability to visibility, the user is in control with no control. Based on the limited use of active hours reported by our participants, an alternative may be for Windows to learn sensible defaults from usage activity and set appropriate restart times automatically. This suggests a strand of further work to anticipate reactions to updates from prior and current interactions with the computer, rather than with updates specifically.

In order to achieve a more usable update experience, while at the same time allowing system updates and subsequent restarts to occur without disruption of running applications, application code will have to be changed. Encouraging developers of applications for the Windows platform to implement APIs is non-trivial, but would help to limit the impact of restarts, and how predictable the outcomes of updates appear for users of Windows 10 Home Edition.

Future research on software updates needs to reflect their changing nature, potentially through combinations of methods as demonstrated here. As updates become more silent and humans are taken out of the loop, the enactment of secure behaviours is no longer solely down to the user. This shift will require new incentives for secure behaviour as the ecosystem becomes more homogeneous and the potential impact of bugs and vulnerabilities increases.

Data availability

The full survey text is available in Appendix and can also be found alongside anonymous participant responses at doi:10.14324/000.ds.10066165.

Acknowledgements

We would like to thank our previous reviewers as well as Tristan Caulfield for constructive, detailed feedback. This work was supported by the Engineering and Physical Sciences Research Council [grant number EP/P011896/2].

Appendix

This appendix lists the full survey instrument. Note Q1 has been omitted from this listing as it is an administrative question for the Prolific survey platform. The original numbering has been maintained for consistency. All text below appeared in the survey. The screenshots appeared immediately after the question. Where the caption of a screenshot describes the content of the screenshot, this description was also included in the survey text. Where there is no description present, none was given in the real survey either.

Q2. Have you ever worked or studied for a qualification in a computer-related field?

For example, answer 'Yes' if you have studied computer science at school or college or if you have worked in a computing-related field such as computer programming, IT management or computer networking. (Compulsory, choose one)

- Yes
- No

Q3. Which of these answers best describes who takes responsibility for the maintenance of your computer?

Maintenance includes things like installing new applications or creating new accounts for additional people to use your computer. 'Other people' might be a family member, friend or a shop or call centre worker who provides you with a technical support service. (Compulsory, choose one)

- I do all of the maintenance myself
- I do most of the maintenance myself but occasionally seek help from other people
- I leave most of the maintenance to other people
- I leave all the maintenance to other people
- Not sure

Q4. Please describe your level of experience in each of these versions of Windows?

(Compulsory, select for each item from: Used Extensively/Used moderately/Used a little/Not used/Not sure)

- Windows 95
- Windows 98
- Windows ME
- Windows Vista
- Windows 7
- Windows 8
- Windows 10

New survey page

Q5. Do you use your computer for any of the following purposes?

(Optional, multiple choice)

- Using websites
- E-mail
- Gaming
- Running 'office' applications e.g. word processing, spreadsheets and presentations
- Online banking
- Online shopping
- Social media
- Video conferencing, e.g. Skype

Q6. Thinking of the things you use your computer for and using the 5-point scale below, how would you describe… (Compulsory, select for each item from Very slow/Slow/Neither noticeably slow nor noticeably fast/Fast/Very fast)

- the speed of your computer

Q7. Do you share your computer with other people? (Compulsory, choose one)

- Yes, there is at least one other person in my household who uses it regularly
- Yes, there is at least one other person outside my household who uses it regularly.
- Yes, there is at least one other person in my household and at least one other person outside my household who uses it regularly.
- No, I am the only person who uses it regularly

Q8. Which answer best describes what happens to your computer when no one is using it? (Compulsory, choose one)

It is left on all the time
It is left on all the time but the screen switches off after a period of inactivity.
It is put into 'sleep' mode
It is put into 'hibernate' mode
It is 'shut down'
I do something else
I am not sure

Q9. Approximately how many days each week is your computer used? (Compulsory, choose one)

- At least once a day
- 5–6 days each week
- 2–4 days each week
- At most once a week

Q10. Do you typically use your computer on weekdays? (Compulsory, choose one)

- Yes
- No

Q11. On weekdays when you use your computer, when do you typically use it?

(Compulsory, multiple choice, shown if answer to Q10 is 'Yes')

- Between 2 am and 5 am
- Between 5 am and 8 am
- Between 8 am and 11 am
- Between 11 am and 2 pm
- Between 2 pm and 5 pm
- Between 5 pm and 8 pm
- Between 8 pm and 11 pm
- Between 11 pm and 2 am

Q12. Do you typically use your computer on weekends? (Compulsory, choose one)

- Yes
- No

Q13. On weekends when you use your computer, when do you typically use it?

(Compulsory, multiple choice, shown if answer to Q12 = 'Yes')

- Between 2 am and 5 am

- Between 5 am and 8 am
- Between 8 am and 11 am
- Between 11 am and 2 pm
- Between 2 pm and 5 pm
- Between 5 pm and 8 pm
- Between 8 pm and 11 pm
- Between 11 pm and 2 am

Q14. Approximately how long have you had your computer? (Compulsory, choose one)

- Less than a month
- Between a month and 6 months
- Between 6 months and 1 year
- Between 1 and 2 years
- Between 2 and 3 years
- 3 years or more

Q15. My computer is. . . (Compulsory, choose one)

- A laptop computer
- A desktop computer
- A tablet computer
- A combined laptop/tablet computer
- Not sure

New survey page

Q16. How frequently do you believe each of the following statements about software updates for the Windows 10 operating system is true?

(Compulsory, select for each item from: Always/Often/Occasionally/Rarely/Never/Don't Know)

- They fix errors in the software on my computer
- They introduce errors into the software on my computer
- They help to keep me safe
- They change the appearance of my system
- They introduce new features
- They remove features
- They stop other software on my computer from working
- Microsoft charge me for them
- They are installed automatically
- Please select 'Never' as the answer to this question
- My computer needs to be restarted when updates are installed
- My computer asks for my permission before it restarts to install an update

Q17. Which answer best describes how often you believe new updates for your Windows 10 computer are released? (Compulsory, choose one)

- There is a new update every 6 months
- There is a new update every 2 months
- There is a new update every month
- There is a new update every week
- There is a new update every day
- Not sure

New survey page

Q18. To what extent do you agree or disagree with each of the following statements?

(Compulsory, delect for each item from: Strongly agree/Agree/Neither agree or disagree/Disagree/Strongly disagree)

- My computer could be affected by cybercriminals
- The data on my computer would be of value to cybercriminals
- My online data would be of value to cybercriminals
- My computer could be used by cybercriminals to affect other people
- Websites I use could be attacked by cybercriminals

New survey page

Q19. Is the message shown in Fig. A1 familiar to you?
[Fig. A1 about here.]
(Compulsory, choose one)

- Yes, I have seen this message before
- No, I don't recall seeing this message before
- Not sure

Q20a. Think back to what you have done in the past when you have seen this message. If you are in the middle of an hour-long task on your computer that is important to you when the message appears, which answer best describes how you would typically respond?

(Compulsory, choose one, shown if answer to Q19 = 'Yes')

- I would ignore the message because I don't understand it
- I would press 'Restart now'
- I would press 'View Settings'
- I would make a special point of 'restarting' later myself after my task is complete
- I would choose to 'Update and shut down' later when I have finished using my computer
- I would leave my computer to restart on its own later
- I would ask someone else for advice about what to do next

Q20b. If you are in the middle of an hour-long task on your computer that is important to you when the message appears, which answer best describes how you would expect to respond? (Compulsory, choose one, shown if answer to Q19 = 'No' or 'Not sure')

- I would ignore the message because I don't understand it
- I would press 'Restart now'
- I would press 'View Settings'
- I would make a special point of restarting my computer myself after my task is complete
- I would choose to 'Update and shut down' later when I have finished using my computer
- I would leave my computer to restart on its own later
- I would ask someone else for advice about what to do next

Q21. Approximately how much time would you expect the restart required by this update to take on your computer? (Compulsory, choose one)

- Less than 5 min
- 5–14 min
- 15–29 min
- 30–44 min
- 45–59 min
- 60–89 min
- 90–119 min
- 2 h or more

Q22. To the best of your knowledge, has your computer ever restarted to install an update unexpectedly? (Compulsory, choose one)

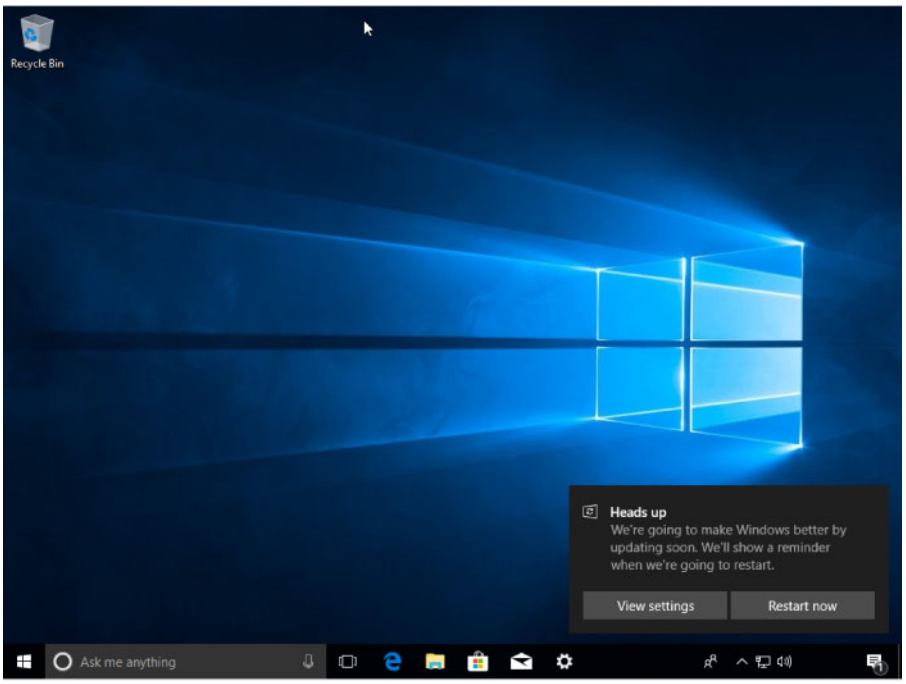

Figure A1: Screenshot of Windows for Q19. The message in the image reads: 'Heads up. We're going to make Windows better by updating soon. We'll show a reminder when we're going to restart.' The two buttons are labelled 'View settings' and 'Restart now'.

- Yes
- No
- Not sure

Q23. How would you describe the behaviour of your computer when it restarted unexpectedly? (Compulsory, choose at most three, shown if answer to Q22 = 'Yes')

- Disruptive
- Inconsiderate
- Inflexible
- Prudent
- Cautious
- Necessary
- Protective
- Clever
- Forward-thinking

New survey page

Q24. Like the last section, imagine you are using your computer to work on a task that is important to you when a message like the one in Fig. A2 appears. You must choose an option before you can resume your work. What would you choose to do?

[Fig. A2 about here.]

(Compulsory, choose one)

- Press 'Pick a time'
- Press 'Remind me later'
- Press 'Restart now'

Q25. How would you eventually choose to restart your computer?

(Compulsory, choose one, shown if answer to Q24 = 'Remind me later')

- I would make a special point of restarting my computer myself after my task is complete
- I would choose to 'Update and shut down' when I have finished using my computer
- I would eventually 'Pick a time' and leave my computer to automatically restart itself
- I would ask someone else for advice
- I would do something else

Q26. Approximately how much time would you expect this restart to take on your computer? (Compulsory, choose one)

- Less than 5 min
- 5–14 min
- 15–29 min
- 30–44 min
- 45–59 min
- 60–89 min
- 90–119 min
- 2 h or more

New survey page

Q27. Sometimes when an update is being installed, a 'Working on Updates' or 'Configuring updates' screen like the one in Fig. A3 is displayed. Is this screen familiar to you?

[Fig. A3 about here.]

(Compulsory, choose one)

- Yes, I have seen this screen before
- No, I have not seen this screen before
- Not sure

Q28. To what extent do you agree or disagree with the following statements?

(Compulsory, select for each item from: Strongly agree/Agree/Neither agree or disagree/Disagree/Strongly disagree, only shown if answer to Q27 = 'Yes')

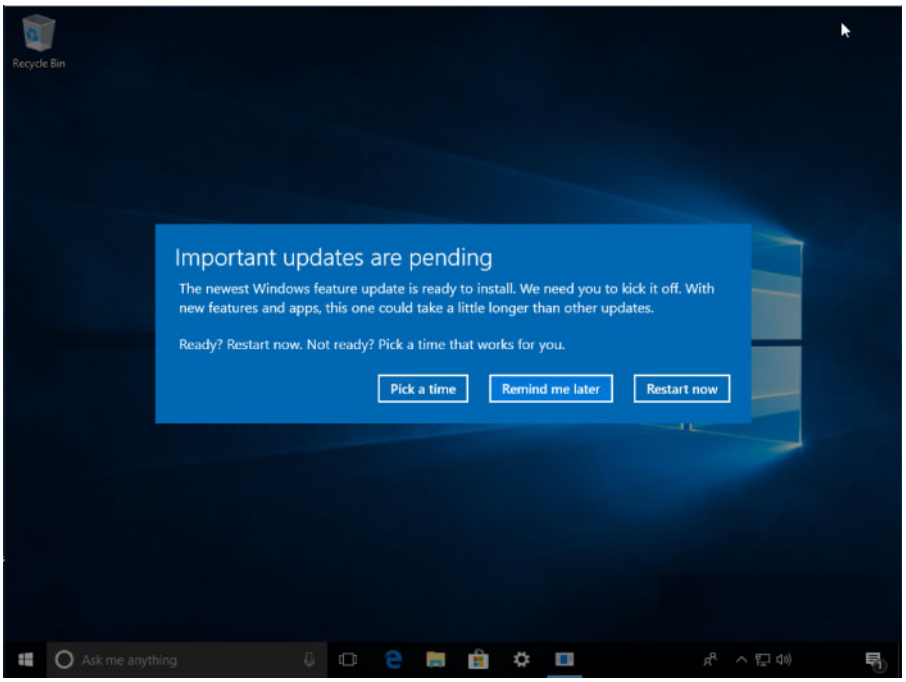

Figure A2: Screenshot of Windows for Q24. The message in the image reads: 'Important updates are pending. The newest Windows feature update is ready to install. We need you to kick it off. With new features and apps, this one could take a little longer than other updates. Ready? Restart now. Not ready? Pick a time that works for you.' The buttons are labelled 'Pick a time', 'Remind me later' and 'Restart now'.

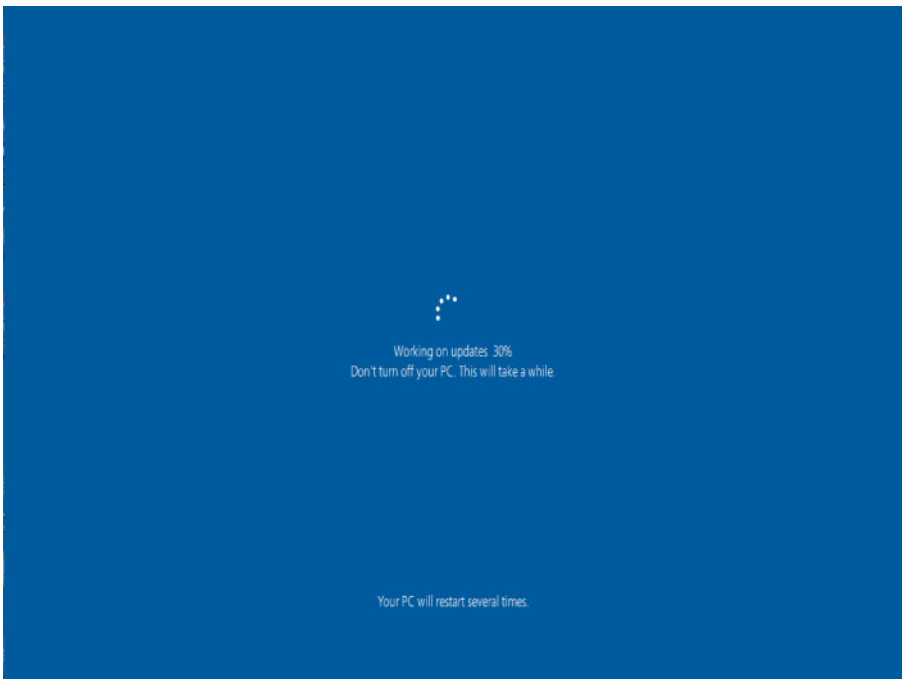

Figure A3: Screenshot of Windows for Q27.

- This screen gives me helpful information about the update's progress
- The longer this screen appears the more concerned I become

New survey page

Q29. To what extent do you agree or disagree with each of the following statements?

(Compulsory, select for each item from: Strongly agree/Agree/Neither agree or disagree/Disagree/Strongly disagree/Not sure)

- My computer gives me sufficient warning about its need to restart to install an update
- When my computer restarts to install an update, I worry it won't work afterward

- When my computer installs an update, I need to devote time to getting familiar with any changes the update introduces
- When my computer restarts to install an update, I have to spend time reopening my applications before I can resume where I left off
- I can sufficiently control when my computer restarts for the installation of an update
- My computer asks me to restart to install updates too frequently
- Please select 'Neither' as the answer to this question
- Aside from the need to restart to complete the installation of an update, I don't notice updates being downloaded and installed on my computer

Q30. Restarting my computer to complete the installation of an update takes...
(Compulsory, select one)

- A lot more time than I expect
- More time than I expect
- About the amount of time I expect
- Less time than I expect
- A lot less time than I expect
- Don't know

Q31. To what extent do you agree or disagree with each of the following statement?
(Compulsory, select for each item from: Strongly agree/Agree/Neither agree or disagree/Disagree/Strongly disagree, Only shown if answer to Q4 reports 'extensive' or 'moderate experience' of any version of Windows prior to Windows 10)

- Updating Windows 10 is easier than previous versions of Windows
- Updating Windows 10 does not interrupt my work as much as previous versions of Windows

Q32. Windows limits the software updates it downloads and installs to the most important ones if the current network connection has been marked as 'metered'. Have you ever marked a connection as 'metered' only because you wanted to reduce the number of updates installed?
A metered network connection is one where the more it is used, the more you are charged, e.g. mobile/cellular networks may charge on this basis. Thus by limiting the number of software updates that are downloaded, Windows tries to limit the charges. (Compulsory, select one, shown if answer to Q3 is 'all' or 'most' maintenance myself)

- Yes
- No
- Not sure

New survey page
Q33. Windows 10 allows users to proactively check for new updates by pressing the 'Check for updates' button in the 'Settings' application (as seen in Fig. A4). If any are found, it will immediately download and install them. Have you proactively checked for updates in the past?
[Fig. A4 about here.]
[Compulsory, Select one]

- Yes
- No
- Not sure

Q34. Why have you proactively checked for updates in the past?
(Compulsory, multiple choice, shown if answer to Q33 is 'Yes')

- Because I have wanted to install an update to fix a security problem I'd heard about
- Because I have wanted to install a new feature update I'd heard about
- Because I have encountered a problem on my computer that I'd hoped an update might fix
- I make it a habit to regularly check for new updates for security reasons
- Because by proactively checking for new updates I can better control when they get installed
- Because I have wanted to check the update system is working correctly.

New survey page
Q35. 'Active hours' is a Windows 10 feature that allows users to specify a period of time when their computer is normally in use. If a software update needs to restart the computer, the computer will avoid restarting it during that period. An image of the screen used to set the feature is shown in Fig. A5. Prior to this survey, were you aware of this feature?
[Fig. A5 about here.]
(Compulsory, select one)

- Yes
- No

Q36. The default setting for 'Active Hours' is from 8 am to 5 pm. To the best of your knowledge, has the 'Active Hours' period been changed on your computer?
By 'default setting', we mean when a new Windows 10 computer is used for the first time, 'Active Hours' will be set to 8 am to 5 pm. You can see the 'Active Hours' period on your computer by opening the 'Settings' application, choosing 'Update & Security' then click on 'Change active hours'. Press the Cancel button to close the window without changing the setting. (Compulsory, select one, shown if answer to Q35 is 'Yes')

- Yes
- No
- Not sure

New survey page
Q37. Windows 10 includes a feature that allows you to limit the amount of your computer's Internet bandwidth that it uses to download software updates. For example, it can be limited to 45% of the available capacity. An image of the screen used to set up the feature is shown in Fig. A6. Prior to this survey, were you aware of this feature?
[Fig. A6 about here.]
(Compulsory, select one, shown if answer to Q3 is 'I do most of the maintenance myself but occasionally seek help from other people' or 'I do all of the maintenance myself')

- Yes
- No

Q38. Have you used this feature?
(Compulsory, select one, shown if answer to Q37 is 'Yes')

- Yes
- No
- Not sure

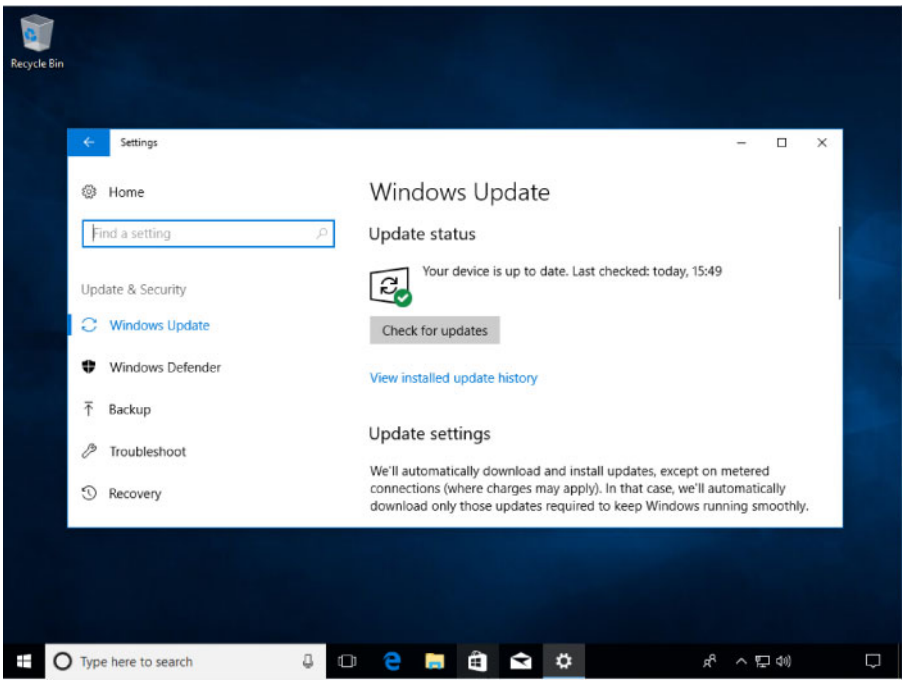

Figure A4: Screenshot of Windows for Q33.

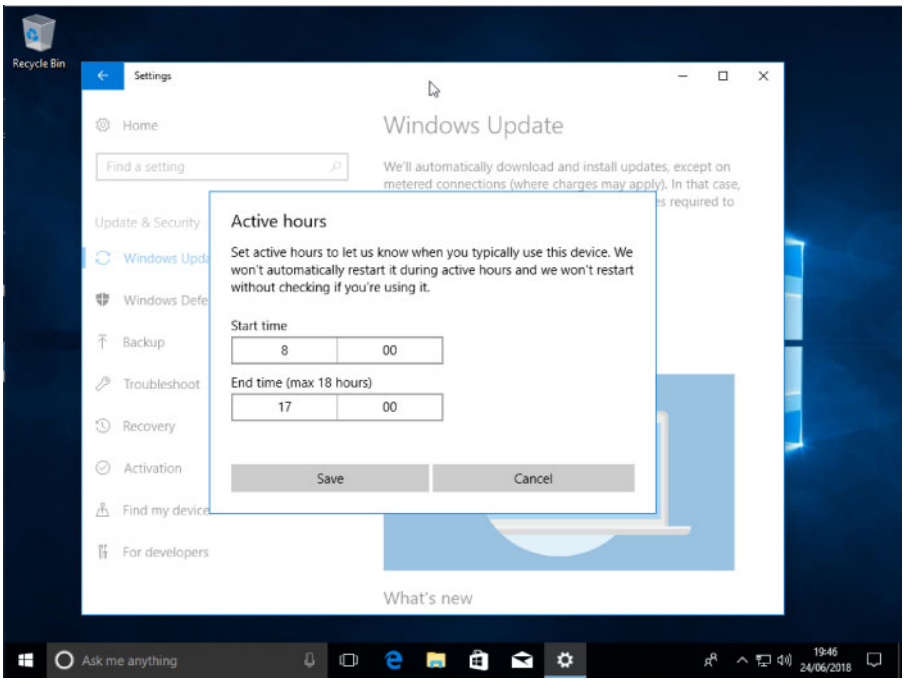

Figure A5: Screenshot of Windows for Q35.

New survey page

Q39. Windows 10 includes a 'Windows Update Trouble-shooter' for identifying and fixing problems with the installation of updates. An image of the screen used to run the trouble-shooter is shown in Fig. A7. Prior to this survey, were you aware of this feature?

[Fig. A7 about here.]

(Compulsory, Select one, Shown if answer to Q3 is 'I do most of the maintenance myself but occasionally seek help from other people' or 'I do all of the maintenance myself')

- Yes
- No

Q40. Have you tried to use this feature?

(Compulsory, Select one, Shown if answer to Q39 is 'Yes')

- Yes
- No
- Not sure

New survey page

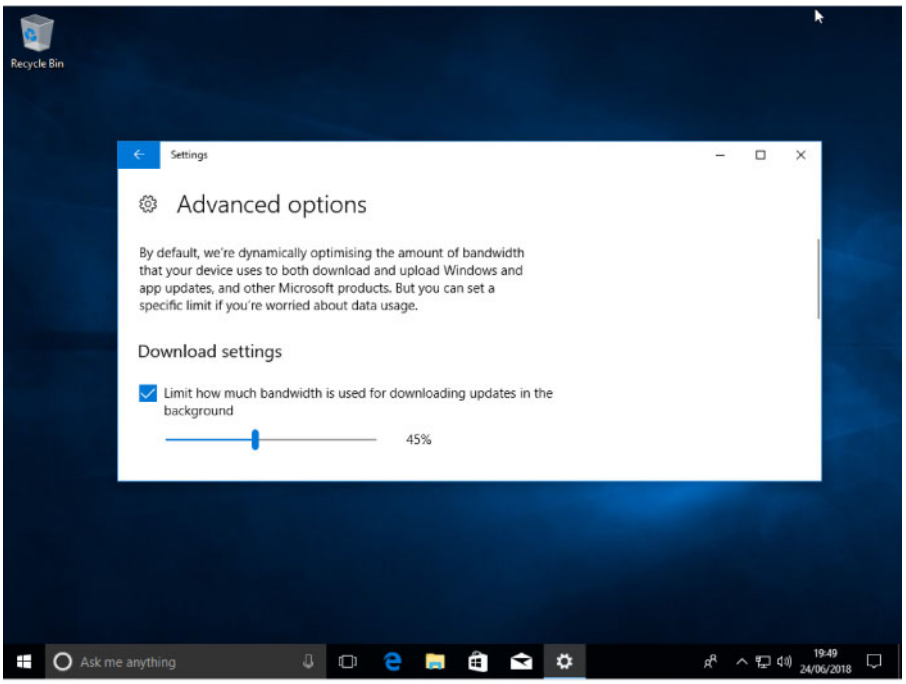

Figure A6: Screenshot of Windows for Q37.

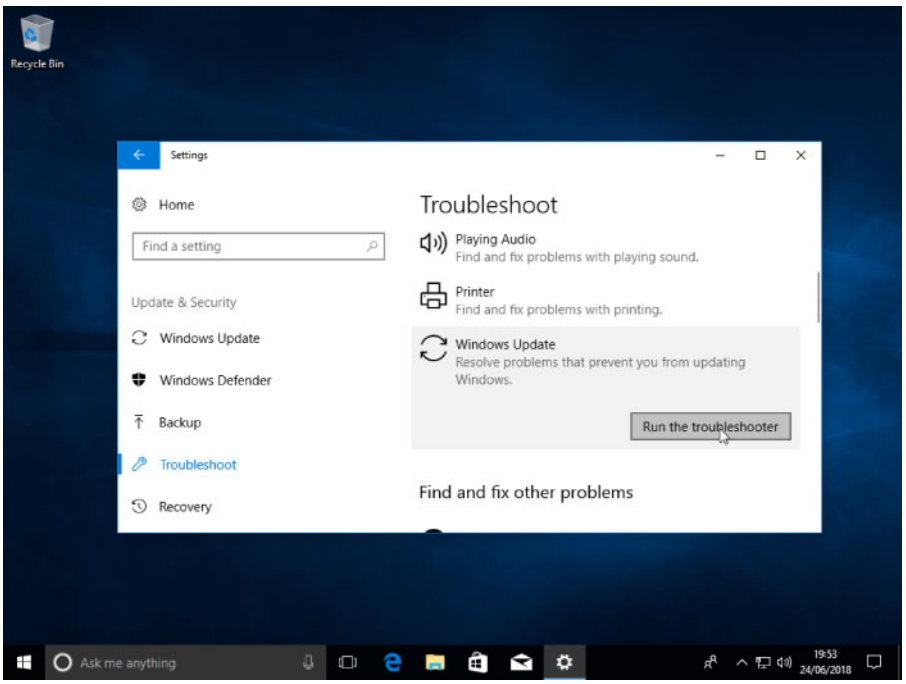

Figure A7: Screenshot of Windows for Q39.

[Fig. A8 about here.]

Q41. Windows 10 includes a feature that allows an update to be uninstalled. You might consider doing this if you suspect a specific update caused a problem with your computer. An image of the screen for the feature is shown in Fig. A8. Prior to this survey, were you aware of this feature?

(Compulsory, select one)

- Yes
- No

Q42. Have you used this feature?

(Compulsory, Select one, Shown if answer to Q41 is 'Yes')

- Yes
- No
- Not sure

New survey page

Q43. To what extent do you agree or disagree with each of the following statements?

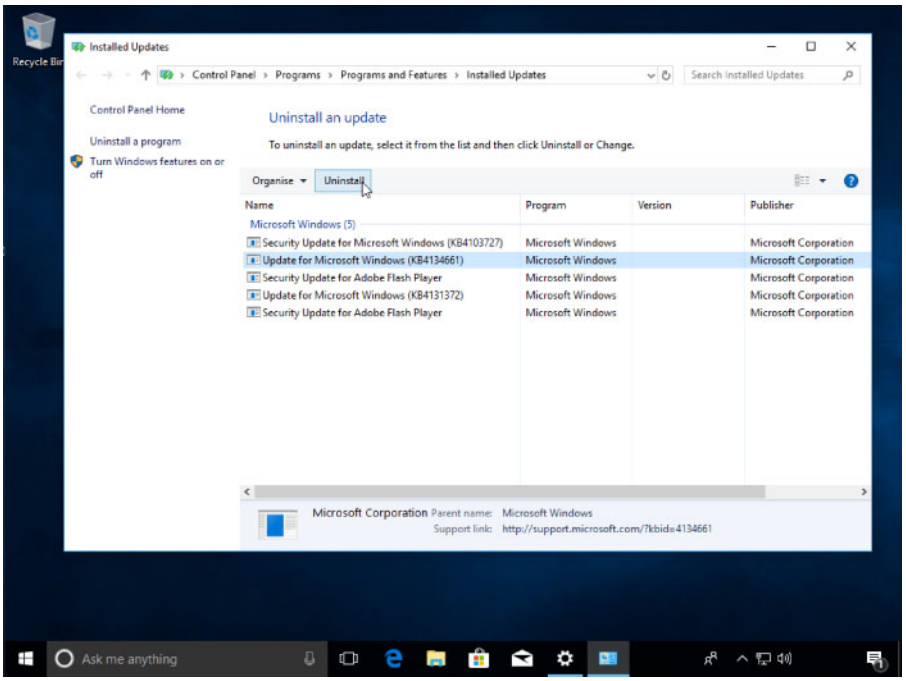

Figure A8: Screenshot of Windows for Q41.

(Compulsory, select for each item from: Strongly agree/Agree/Neither agree or disagree/Disagree/Strongly disagree)

- I trust Microsoft to provide the updates for their software I need to keep my computer safe
- I trust other software producers to provide the updates for their software I need to keep my computer safe
- Updates are convenient
- Updates keep me safe

Q44. How certain are you of the accuracy of your responses to this survey?

(Compulsory, select one)

- Uncertain/guessing
- Mostly uncertain
- Mostly certain
- Certain

Thank you for participating!

References

1. Ioannidis C, Pym D, Williams J. Information security trade-offs and optimal patching policies. *Eur J Oper Res* 2012;**216**:434–44.
2. Frei S. The Security Exposure of Software Portfolios. Secunia Tech Rep 2010. https://techzoom.net/static/whitepapers/software_portfolio.
3. Vaniea KE, Rader E, Wash R. *Betrayed by Updates: How Negative Experiences Affect Future Security*. In HI '14: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM Press, Toronto, Ontario, Canada, 2014, pp. 2671–2674. doi 10.1145/2556288.2557275.
4. Vaniea KE. *Human Factors of Software Updates - Microsoft Research Presentation*, 2015. http://www.talks.cam.ac.uk/talk/index/60736.
5. Ion I, Reeder R, Consolvo S. "... No one can hack my mind": comparing expert and non-expert security practices. *SOUPS* 2015;**15**:1–20.
6. Dodier-Lazaro S, Becker I, Krinke J *et al.* No good reason to remove features: expert users value useful apps over secure ones. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Cham: Springer, 2017, pp. 25–44.
7. Mathur A, Malkin N, Harbach M *et al. Quantifying Users' Beliefs about Software Updates*. Internet Society, San Diego, CA, USA, 2018. doi: 10.14722/ndss.2018.23036.
8. Herley C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In: *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, ACM, 2009, pp. 133–144.
9. Duebendorfer T, Frei S. *Why Silent Updates Boost Security*. ETH Zurich, Technical Report 302, 2009.
10. Frei S, Duebendorfer T, Plattner B. Firefox (in) security update dynamics exposed. *ACM SIGCOMM Comp Commun Rev* 2008;**39**:16–22.
11. Beautement A, Sasse MA, Wonham M. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*, ACM, Lake Tahoe, California, USA, 2009, pp. 47–58.
12. Herley C. More is not the answer. *IEEE Secur Priv* 2014;**12**:14–19.
13. Decker U. *Windows 10 - Prevent Auto-Reboot after Installing Updates (Anniversary Update)*, 2017. https://www.udse.de/en/windows-10-reboot-blocker (1 July 2018, date last accessed).
14. pf100. Sledgehammer. version 2.7.0, 2020. https://forums.mydigitallife.net/threads/sledgehammerwindows-10-update-control.72203/(26 March 2020, date last accessed).
15. Wash R, Rader E, Vaniea K *et al.* Out of the loop: how automated software updates cause unintended security consequences. In: *Symposium on Usable Privacy and Security (SOUPS)*, USENIX Association, 2014, pp. 89–104.
16. Bergman O, Whittaker S. The cognitive costs of upgrades. *Interact Comput* 2018;**30**:46–52.
17. Fagan M, Khan MMH, Nguyen N. How does this message make you feel? A study of user perspectives on software update/warning message design. *Hum-Cent Comput Info Sci* 2015;**5**:3.
18. Mathur A, Chetty M. Impact of user characteristics on attitudes towards automatic mobile application updates. In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, OCLC: 255559492, Santa Clara, CA, ISBN: 978-1-931971-39-3.
19. Farhang S, Weidman J, Kamani MM *et al.* Take it or leave it: a survey study on operating system upgrade practices, 2018, p. 16. 10.1145/3274694.3274733.

20. Edwards WK, Poole ES, Stoll J. Security automation considered harmful? In: *Proceedings of the 2007 Workshop on New Security Paradigms*, ACM, New Hampshire, USA. 2008, pp. 33–42.
21. Wash R, Rader E. Influencing mental models of security: a research agenda. In: *Proceedings of the 2011 New Security Paradigms Workshop*, ACM, Marin County, California, USA, 2011, pp. 57–66.
22. Krol K, Spring JM, Parkin S *et al.* Towards robust experimental design for user studies in security and privacy. In: *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2016), USENIX Association*, 2016, pp. 21–31.
23. Thapar G, Li J, Ramlan S. Initiating update operations. US9405526B2, 2016. https://patents.google.com/patent/US9405526B2/en.
24. Forget A, Pearman S, Thomas J *et al.* Do or do not, there is no try: user engagement may not improve security outcomes. In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, USENIX Association, 2016, pp. 97–111, ISBN: 978-1-931971-31-7.
25. Redmiles EM, Kross S, Mazurek ML. How I learned to be secure: a census-representative survey of security advice sources and behavior. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, Vienna, Austria, 2016, pp. 666–677.
26. Furnell S, van Niekerk J, Clarke N. The price of patching. *Comput Fraud Secur* 2014;**2014**:8–13.
27. Conway J. We're Listening to You—Feature Update Improvements, 2018. https://insider.windows.com/en-us/articles/were-listening-to-you/ (1 July 2018, date last accessed).
28. Wash R. Folk models of home computer security. In: *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM,Redmond, Washington, USA, 2010, p. 11.
29. Vaniea K, Rashidi Y. Tales of software updates: the process of updating software. In: *Proceedings for Computer Human Interaction (CHI) 2016*. San Jose, CA: ACM Press, 2016, pp. 3215–26.
30. Vitale F, McGrenere J, Tabard A *et al.* High costs and small benefits: a field study of how users experience operating system upgrades. In: *CHI 2017*, Denver, CO: ACM, 2017, pp. 4242–4253.
31. Mathur A, Engel J, Sobti S *et al.* "They keep coming back like zombies": improving software updating interfaces. In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. OCLC: 255312726, Denver, CO: Usenix Association, 2016.
32. Microsoft. *Registering for Application Restart (Windows)*, 2018. https://docs.microsoft.com/engb/windows/desktop/Recovery/registering-for-application-restart (1 July 2018, date last accessed).
33. Google Android. *Understand the Activity Lifecycle*, 2019. https://developer.android.com/guide/components/activities/activity-lifecycle (23 May 2019, date last accessed).
34. Google. *Update Your Chromebook's Operating System - Chromebook Help*, 2014. https://support. google.com/chromebook/answer/177889?hl=en-GB (3 October 2018, date last accessed).
35. Constantine LL, Lockwood LA. *Software for Use*. ACM Press/Addison-Wesley, New York, NY, US, 1999.
36. Cable J. *Updated Version of Windows 10 October 2018 Update released to Windows Insiders*, 2018. https://blogs.windows.com/windowsexperience/2018/10/09/updated-version-of-windows-10-october-2018-updatereleased-to-windows-insiders/(23 November 2018, date last accessed).
37. Wash R, Rader EJ. Too much knowledge? security beliefs and protective behaviors among United States internet users. *SOUPS* 2015: 309–25. https://www.usenix.org/conference/soups2015/proceeding.