Betrayed By Updates: How Negative Experiences Affect Future Security

ABSTRACT

Installing security-relevant software updates is one of the best computer protection mechanisms. However, users do not always choose to install updates. Through interviewing non-expert Windows users, we found that users frequently decide not to install future updates, regardless of whether they are important for security, after negative experiences with past updates. This means that even non-security updates (such as user interface changes) can impact the security of a computer. This update behavior is becoming increasingly important as devices move toward an "app" model for software distribution and updates.

INTRODUCTION

Software companies regularly release updates that are intended to improve upon previously installed programs. These improvements can range from invisible but necessary changes, like small bug fixes and security patches, to significant feature changes that affect user workflow. Security updates are particularly important because they are one of the primary mechanisms users have at their disposal to protect their computers from malicious software that leverages known vulnerabilities. As soon as a vulnerability becomes public knowledge, malicious software authors begin writing code that uses the vulnerability to compromise computers, so timely installation of security updates can protect a computer from these attacks [1]. Both Symantec and Microsoft have observed that the majority of computers are compromised using vulnerabilities for which a security update is available but has not yet been installed [3, 7]. Timely installation of security updates can protect users from the most common attacks [7].

However, some updates combine security and non-security components, and it is not always clear to users which updates will improve security and which updates might make other changes. Some software updates are *technically* cumulative: all prior updates must be installed before the latest update can be installed. This means that security updates cannot be installed until the user decides to install earlier, non-security updates. This lack of differentiation, and the decisions companies make about how to roll out non-security updates, combined with the decisions users make about whether to install these updates, can potentially affect the overall security of users' computers.

We interviewed Windows users about their opinions and beliefs concerning software updates, to understand what makes people not want to update software. We found that respondents avoided updates that caused unexpected user interface changes. They also felt less inclined to update software they perceived as currently functional, or that they rarely used or saw in action. These attitudes were learned over time from previous experiences with software updates, and stemmed from a desire to avoid risky actions with the potential to interfere with their workflow. Given the rise of the "app" model of software distribution [5], users are now encountering more and more update notifications, and must make increasingly frequent decisions about whether or not to update. This presents a new challenge for software update authors, who should no longer assume that update compliance occurs in a vacuum.

METHOD

We recruited 37 non-expert Windows 7 users to participate in a study about software updates by sending an email through the Registrar of a large public university to a random sample of non-technical graduate students. Respondents were screened to ensure they used Windows 7 and had no prior experience in Computer Science or professional Windows management. Respondents ranged from 21 to 57 years old, with an average age of 31; 17 were male and 20 were female. Three respondents were Mac users running Windows 7 in a virtual machine.

Software updates occur intermittently, and often while users are otherwise occupied; we therefore used retrospective, semi-structured interviews in which respondents were asked wide-ranging questions intended to elicit stories about past experiences with software updates. The interviewer presented each respondent with five software update scenarios and probed for past experiences with the scenario, associated problems or outcomes, and opinions about the scenario.

Interview sessions lasted around one hour, and respondents were compensated $25. Interviews were recorded, transcribed, and scrubbed to remove any personally identifying information. Each respondent was assigned a pseudonym, and we refer to individuals by their pseudonyms below. One member of the research team analyzed the interviews using an open, inductive approach, starting with an initial list of themes identified by the interviewers. The research team held regular meetings in which we discussed and iterated on the codes that emerged, and then expanded and modified the codes as we read through transcripts. In later stages of the analysis, high-level themes emerged as we made connections between codes and participants [4].

Submitted for review to CHI 2014.

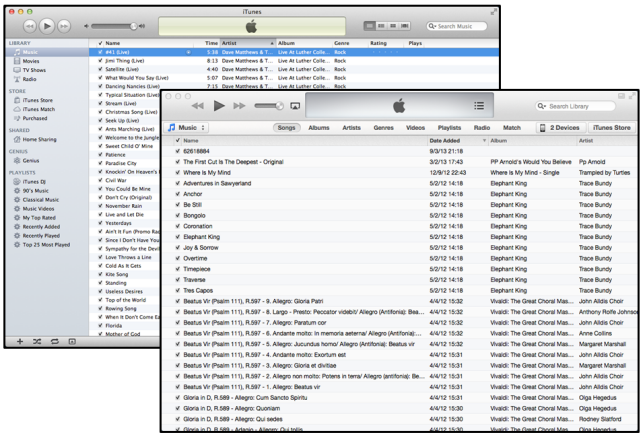

Figure 1. iTunes user interface for version 10.7 (top left) contains a navigation bar on the left, and in version 11 (bottom right) the navigation bar can only be accessed via a menu button.

FINDINGS

Our respondents talked about three overall themes for reasons they did not install software updates: trepidation about surprise new features in an update; the difficulty of assessing whether an update is "worth it" given uncertainty about what a program does and why it is needed; and confusion about why an update is necessary, if the program seems to be working fine. We discuss each theme in the context of a different piece of software that illustrates both the reason for not updating and the security implications.

Surprise UI Changes: "Just, like, leave it alone..."

User interface changes were disruptive for respondents' workflows, and were commonly mentioned. They found new interfaces "annoying" to learn, and reported that they avoided updating software that had a history of frequently changing the user interface. For example, Nick discussed how new user interfaces were hard to learn and made him reluctant to update:

> "I just hate the idea of having to just relearn everything, where everything is, how to access 'help', something as basic as that. And when the new Office suite came along with Excel especially. Word, bad; Excel, worse, as far as just being completely different, counter-intuitive. I try to stick with what I know rather than just take the time to relearn a whole new system."

In addition to being annoying, user interface changes were perceived to have an immediate, negative impact on productivity. Kim talked about how she had "been working with these programs for 15 years. I know them like the back of my hand." To interact with the programs quickly Kim learned the hot keys, specific combinations of keyboard keys that can be used instead of clicking buttons on the user interface. However, "every now and again, you get a new version and they change the hot keys."

The impact of interface changes on respondents' willingness to install current and future updates was particularly highlighted by changes Apple made in version 11 of iTunes, their multimedia player. In iTunes version 10.7 the user interface had a navigation sidebar permanently visible on the left side of the screen. However, version 11 removed the navigation, and the user interface became modal with different available actions depending on the type of content being viewed (Figure 1).

The version 11 update was very unpopular with our respondents. Ashley expressed a common reaction: "all of a sudden, like, *Where did my things go?*" Respondents installed the update not realizing that the user interface was going to change, and then became upset when it did. This caused some respondents to become wary of iTunes updates in general. Amber said that she had "ignored [iTunes updates] quite a few times because I'm like: *I don't need that update*." Rachel expressed worry about future iTunes updates:

> "I also always worry that everything is gonna get screwed up, especially for iTunes updates or things like that because they're always reconfiguring the layout of stuff, and I'm like, 'I don't want you to do that. Just, like, leave it alone...'"

Some respondents had learned from past experiences to check technology blogs and forums as a way of finding out what new updates might do before installing them. Melissa learned that the iTunes update would change the interface and explained that she had waited to update iTunes because she "was not ready to get used to [the new interface]." Chris talked about deciding not to update iTunes after reading that other people didn't like the new interface.

> "One of the prior iterations of iTunes, it just wasn't well received and there were some... A lot of complaints about the new version. People saying, 'Don't update'. I'm like, okay, I won't update."

Other respondents had less foresight and ended up installing an unwanted iTunes update. In Lauren's case, an update disabled her ability to manage her old iPod. After the loss, Lauren began refusing all iTunes updates because she was "mad at them."

> "You can't update it and and you can't change the songs because the new version of iTunes is like, 'Even though you took really good care of your machinery, we don't want you to have that one anymore.'"

On the surface, iTunes might not seem like it would be associated with security issues, and none of our respondents mentioned any concern about security in relation to iTunes. However, iTunes has the ability to display web pages as part of the iTunes store. Software that displays web pages (HTML/Javascript) is the most common vector for compromise on Windows computers [3]. In its version 10.7 release of iTunes, Apple patched 163 vulnerabilities, the majority of which involved the web page display functionality. Most users don't browse the web using iTunes; rather, they browse the internet using their favorite web browser. But when they click on specially formatted links it can cause iTunes to automatically launch an attempt to display the web content as part of the iTunes store. If a user running the 10.6 version of

iTunes were to click the wrong link it could be used to install any software on the user's computer[1].

Respondents talked about the need to update web browsers like Firefox, and Chrome as a way of protecting themselves from dangers on the internet. But they reported thinking about iTunes as a multimedia player that plays their songs, videos and interacts with their Apple devices. Their update choices were based on how they wanted to interact with the software and the functions they needed.

I Don't Understand It, so I Won't Update It

Respondents differentiated between programs they used regularly and programs they used infrequently, or not at all. They were more inclined to update software they used frequently because they recognized that doing so would bring them the latest features and make it easier to interact with other people who were running updated versions of software. They were less inclined to update rarely used software unless there was a good reason. If a program stopped being used entirely, they tended to either stop updating it or uninstall it completely.

Java is a program that provides functionality to other programs installed on a computer. Users rarely, if ever, directly interact with Java even though they may frequently use programs that need Java to function. Java is the second most common source of security compromise on Windows computers, and one of the least updated programs with only 6% of Windows computers running the latest version [3].

Java was problematic for our respondents, because they didn't understand what it was, and they didn't think they used it. Amy's experience highlights the confusion:

> "It's annoying and I don't think I need Java, so I just deleted the program. However, when I visit some website they asked me to install Java. 'Okay. I will install it, but if you ask me to update again, I will delete you."'

To correct several serious security issues, four Java updates were released in six weeks in the beginning of 2013 just before our study. Typically Java releases updates about once every two months, and this escalation may have contributed to our respondents' irritation. Some respondents had formed a general animosity against Java because of the constant requests for updates. They reported feeling that Java wanted to update "all the time" and was really annoying. Lauren didn't understand why she needed Java, and got irritated by the repeated requests to update:

> "I don't know why the hell I need a Java so I ignore it... I'm just pissed off and I think I have a tendency then, when like I see Java pop up in the corner, I'm like, 'Fuck you, Java."'

When respondents became confused by repeated requests for Java updates they said they went online and attempted to understand what the updates were doing. Because Java is well known as being vulnerable to security compromise some online forms advise uninstalling it. However, it is necessary for many programs to function correctly, so other forums recommend updating it regularly. Respondents searching for information on Java encountered conflicting discussions similar to the rhetoric described above and became confused about what to do. Ashley talked about such an event:

> "I started to think there was a problem, and so then I started looking more, and actually reading to try to decide, do I wanna install the update? You know, some things, [you should] install the update because it will make it better. Other things are like... Just take it off your computer completely."

Because it runs invisibly in the background, our respondents only saw that Java updates costed them time. They didn't understand that updating Java made other programs potentially run better, or that not updating Java made them vulnerable to attackers.

If it Ain't Broke, Don't Fix It!

Respondents explained that if their software was working and fulfilling their needs, they saw no need to make changes. They were reluctant to expend effort and risk problems just to change the behavior of functional software.

As described above, respondents felt updating software is potentially fraught with uncertainty. Most updates provide little to no information to end users about what will occur when they click the "Install" button. In addition to the risk of user interface changes, there is also a risk that a needed feature will be removed from the software, or that the software will stop functioning entirely. When faced with the choice to update users have three options: blindly accept, research, or deny. Accepting the update carries the potential cost of installing an update that has unwanted components, and researching the updates costs time and mental energy, so some respondents chose the least risky option of deny.

Respondents talked about using software until it became non-operational, and then either updating the program or deleting it. Andrew talked about not updating software:

> "Many times I do not update. Just for regular software unless I feel that this software now is not working properly. Otherwise, I'll keep it simple."

Respondents also made a distinction between "regular" software which didn't need to be updated and security software such as anti-virus. Nick talked about how he kept security software up-to-date, but avoided other updates:

> "I feel like if I'm really used to the software I'm using and I think it's meeting my needs I won't upgrade the software. But if it is really important like anti-virus it has to be upgraded."

AdobeReader, a PDF viewer, was an excellent example mentioned by our respondents of a utilitarian software program that had a single clear function, and no obvious link to security. Respondents were puzzled about why AdobeReader needed to be updated at all. Justin explained that he never updated AdobeReader because there was no need to do so: "I just don't see what an update to [AdobeReader] can do. I mean it's PDF files. Its viewing them..." David explained

[1] http://www.zdnet.com/google-helps-close-163-security-vulnerabilities-in-itunes-7000004186/

how he didn't "listen" to AdobeReader update requests, because the current version met his requirements: "Adobe, current version helps me to read. And so that's how I decided my requirements." Respondents saw AdobeReader as fulfilling a specific function, and if it was still functioning they saw no reason to change it.

Respondents talked about updating AdobeReader when it stopped functioning. Part of Mike's job involved downloading PDF files from websites and modifying them. If he did not have the latest version of AdobeReader he could have issues: "If I try and download something that is from a more advanced version, it won't accept it. It'll just die." Nicole also discussed not updating programs like AdobeReader, but when the program stopped opening files she would find and download a new program that wasn't broken.

Document viewers, and AdobeReader in particular, are the third most common source for computer compromises on Windows computers [3]. Respondents thought of document viewers as simply displaying static information; however, they are actually similar to web browsers in that they change the stored information into something visible to the user—a process which can result in security issues.

IMPLICATIONS

Prior work tells us that users don't install updates from all software equally [2, 3]. Our findings show that the decision not to update particular applications is sometimes an intentional one for end users. This decision can leave computers and their users vulnerable to malicious attackers.

We have identified an additional challenge for software updates: people learn from past updates and apply that knowledge when deciding about future updates. When users update a piece of software and have a bad experience, they learn that updates to that software (and possibly updates in general) can have bad effects. Consequently, they may be less inclined to update in the future. Similar to behavior observed by Rader et al. [6], users also look to other people, and particularly blogs and forums, to learn about updates.

Many, but not all, software updates are *technically* cumulative: you cannot install a future update until all past updates are installed. Our findings suggest that many software updates are also *user* cumulative: once a user decides not to install an update, they frequently will avoid future updates for that same piece of software. Also, once a user has a negative experience with an update, they are much less likely to install future updates.

Cumulative updates, due to technical requirements or to user decisions, create problems for security because security-related updates are sometimes avoided—not installed—for non-security-related reasons. For example, when respondents disliked the iTunes 11 interface change, they stopped installing all updates for iTunes, including security patches.

One obvious solution to this is to technically disentangle security updates from other types of updates. If users could install security updates without risking their user interface, features, or being forced to reboot, they might be more inclined to keep software up-to-date. However, most users do not currently distinguish between security updates and feature updates; all updates look the same, and have the same risks. Even if we removed the technical dependency between updates, if users cannot clearly distinguish the two, the cumulative dependency for updates will remain due to user decisions.

The software ecosystem is moving toward a model where apps rather than software suites are the norm, and software created by individuals in their spare time is difficult to distinguish from programs created by large companies with quality assurance departments. Apps bombard users with update notifications, but app updates occasionally introduce new software bugs (such as the recent Google Authenticator bug[2]) that should rightly be avoided, and regularly introduce user interface changes or feature additions. The burden on users to evaluate software updates and decide what to do is increasing. All decisions about updates should be treated as security-relevant, since these decisions will have an important impact on device security.

ACKNOWLEDGMENTS

Removed for blind review.

REFERENCES

1. Bilge, L., and Dumitras, T. Before we knew it: an empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, ACM (New York, NY, USA, 2012), 833–844.
2. Khan, M., Bi, Z., and Copeland, J. Software updates as a security metric: Passive identification of update trends and effect on machine infection. In *Military Communications Conference, MILCOM* (2012), 1–6.
3. Microsoft. Microsoft Security Intelligence Report, Volumne 13, January – June 2012.
4. Miles, M. B., Huberman, A. M., and Saldaña, J. *Qualitative Data Analysis*. A Methods Sourcebook. SAGE Publications, Incorporated, Apr. 2013.
5. Purcell, K. *Half of adult cell phone owners have apps on their phones*. Pew Research Center's Internet & American Life Project, Washington, D.C., Nov. 2011.
6. Rader, E., Wash, R., and Brooks, B. Stories as informal lessons about security. In *SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM (July 2012).
7. Symantec Corporation. Internet Security Threat Report, Volume 18, 2013.

[2]https://support.google.com/accounts/answer/3376859