Betrayed By Updates: How Negative Experiences Affect Future Security

Kami Vaniea, Emilee Rader, Rick Wash
Department of Telecommunication, Information Studies, and Media
Michigan State University
{vaniea, emilee, wash}@msu.edu

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. We discuss three themes impacting users’ willingness to install updates: unexpected new features in an update, the difficulty of assessing whether an update is “worth it”, and confusion about why an update is necessary.

Author Keywords
Software Updates; Human Factors; Security

ACM Classification Keywords
D.2.7 Software Engineering: Distribution, Maintenance, and Enhancement; H.5.2 Information Interfaces and Presentation: User interfaces—user-centered design; K.6.5 Management of Computing and Information Systems: Security and Protection

INTRODUCTION
Software companies regularly release updates that are intended to improve 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 to protect their computers from malicious software. Symantec and Microsoft have observed that the majority of computers are compromised using vulnerabilities for which a security update was available but had not yet been installed [3, 7], making timely installation of security updates important for computer security.

Additionally, 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. 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. The number of “apps” installed by end users is also on the rise [5] resulting in more and more update requests being shown to users. 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 Michigan State 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 a mean age of 31; 17 were male and 20 were female. Three respondents used a Mac with Windows 7 in a virtual machine.

Software updates occur intermittently, and often while users are otherwise occupied; we therefore used retrospective, semi-structured interviews based around a set of hypothetical scenarios to elicit stories about past software update experiences. The interviewer asked participants to imagine how they would respond to: being prompted to restart an internet browser mid-task, seeing that a large number of urgent Windows updates were available, reading a news article about a
version 11 of iTunes, their multimedia player. In 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.

The version 11 iTunes 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 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 installed an unwanted iTunes update. In Lauren’s case, an update disabled her ability to manage her old iPod and caused her to start refusing all iTunes updates because she was “mad at them.”

“You can’t update it 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 it. However, software that displays web pages (HTML/Javascript) is the most common vector for compromise on Windows computers [3] and iTunes displays web pages as part of the iTunes store. 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 use a web browser. But when they click on specially formatted links it can cause iTunes to automatically launch and 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 computer1.

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 without a good reason. If a program stopped being used entirely, they tended to either stop updating it or uninstall it completely. Brandon talked about how update prompts caused him to either remove the program, or find a way to turn off updates.

If I’m not using the program … either the software update will prompt me to go remove the program because I’d say, “I am not using and just get rid of it.” Or, somehow turn off the preferences to say “Don’t remind me to update this” ’cause I am not using the program.

Java in particular was problematic for our respondents, because they didn’t understand what it was, and they didn’t think they used it. 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. 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 websites 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 cost them time. They did not understand that updating Java made other programs potentially run better, or that not updating Java made them vulnerable to attackers. 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].

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:
Many 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 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, unless users can 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 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 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 they will have an important impact on device security.

ACKNOWLEDGMENTS
We thank Zack Girouard and Michelle Rizor for their assistance with data collection and early analysis. We thank everyone associated with the BITLab at MSU for helpful discussions and feedback. This material is based upon work supported by the National Science Foundation under Grant No. CNS-1116544 and CNS-1115926.

REFERENCES
5. Purcell, K. Half of adult cell phone owners have apps on their phones. Pew Research Center’s Internet & American Life Project, Nov. 2011.

\(^2\)https://support.google.com/accounts/answer/3376859