Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences

Michelle Rizor, Kami Vaniea, Emilee Rader, Rick Wash

Software Updates

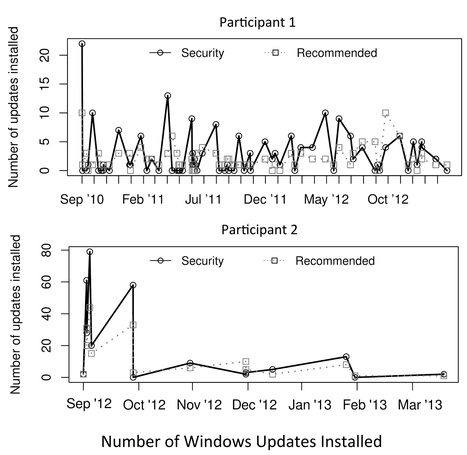
According to Microsoft's Security Report, the majority of computer **compromises** in 2012 could have been **prevented** by timely installation of updates. Many users do not update, or do not update quickly, resulting in increased vulnerability.

Method

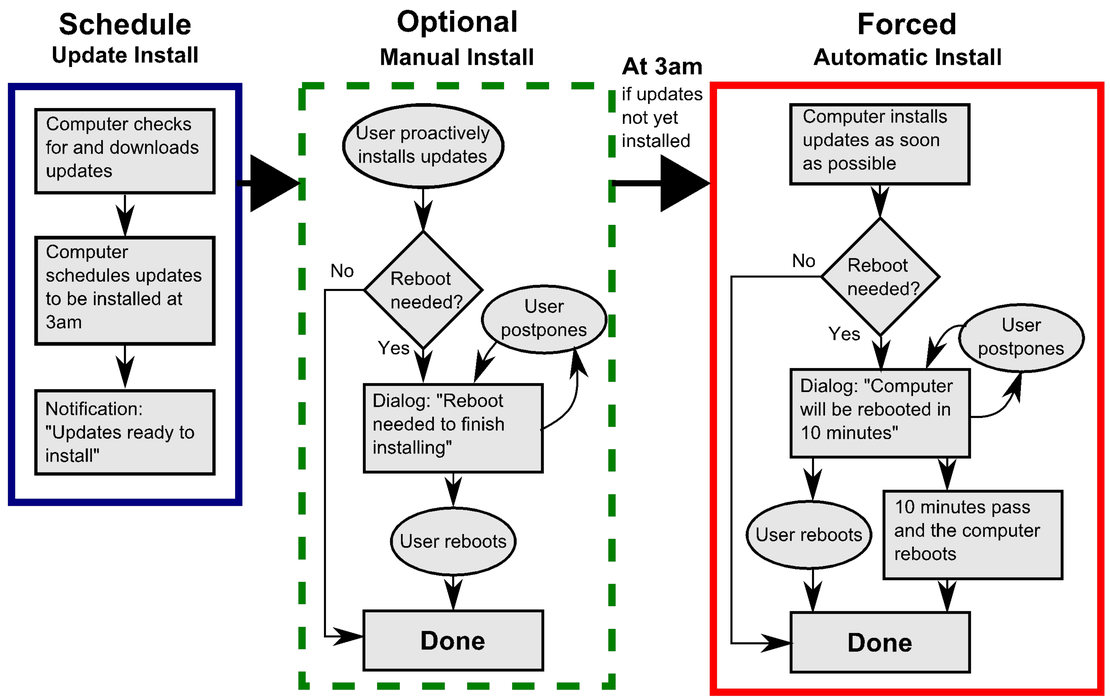
We recruited 37 MSU graduate students who use Windows 7 and are involved in research and utilize CI. This study utilized a multi-method approach with three components:

- Survey
- Semi-structured Interview
- Windows Log Analysis

We compared what users **think** is happening on their computers, what users **want** to happen on their computer, and what was **actually** happening on their computer.



Why Automatic Updates Confuse Users



The process Windows follow to install updates. Windows automatically prepares updates (blue box), then gives users the opportunity to install when convenient for them and to make changes (green box). If the user does not manually install updates (green box), then the system will force installation (red box). This process represents Windows's balance between the needs of the system and the needs of the user.

Software designers have attempted to improve security by automating update processes, effectively removing users from the software update loop.

However, user involvement is still necessary because not all updates are desired, and forced reboots can negatively impact users.

Misunderstandings about update settings

68% of participants were incorrect about their automatic update setting

50% of participants were incorrect about when they install updates

Unable to execute intentions

60% of participants could not act on their intention

60% of participants more secure

40% of participants less secure

Why People Don't Install Updates

Surprise UI changes

User interface changes disrupt workflow and annoy users.

" 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, 'Just, like, leave it alone…' "

Software such as iTunes that can display web pages are the most common vector for compromise.

I don't understand it

Less likely to update software that is perceived to be not frequently used.

" 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, 'F*** you, Java. "

Java is the second most common source for security compromise.

If it ain't broke, don't fix it

If software is working, there is no need to update it.

" 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. "

Document viewers, such as AdobeReader, are third most common source for compromise.

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1116544 and CNS-1115926.