There are really only two effectively distinct settings for the UAC slider

devblogs.microsoft.com/oldnewthing/20160816-00

August 16, 2016

Raymond Chen

There's a control panel that lets you specify how often you want to be prompted by UAC. You can set any of four levels:

- Always notify
- Notify only when apps try to change settings, use the secure desktop
- Notify only when apps try to change settings, don't use the secure desktop
- Never notify

Although it looks like there are four settings, in a theoretical sense, there really are only two settings.

- Always notify
- Meh

The reason why all the other options collapse into *Meh* is that the *Notify only when apps try to change settings* option can be subverted by any app simply by injecting a thread into Explorer and doing its dirty work there. Since Explorer is a program that the setting allows to elevate silently, this lets you perform a silent elevation from any thread that has thread injection rights into Explorer (which is pretty much any program running at medium integrity level or higher).

In other words, *Notify only when apps try to change settings* is really *Punch a hole in the airtight hatchway*.

If the intermediate settings are effectively equivalent to *Never notify*, then why are they there in the first place?

Because people wanted them.

UAC in Windows Vista had only two settings: *Always notify* (enabled, default) and *Never notify* (disabled), because those are the only two meaningful values. But people complained as loudly as they could that the *Always notify* level of prompting was far too annoying.[1] As a concession, Windows 7 introduced two intermediate levels of prompting, even though the two new levels are effectively equivalent to *Never notify* because the notification can be bypassed by a program that puts it mind to it.

As Larry Osterman noted, UAC is not a security feature. It's a convenience feature that acts as a forcing function to get software developers to get their act together.

I remember back in 2009, there was a lot of hubbub over a "security hole" in the UAC control panel because it let you change the UAC settings without prompting, if the old setting was *Notify only when apps try to change settings*.

Well duh.

You configured UAC so that it prompts only if an app is changing a system setting, and not if the control panel itself is changing the setting. You then use the control panel to change a system setting. Therefore, there is no prompt.

Still, enough people complained that they wanted *more prompting* that the UAC folks added an extra prompt. "I thought people complained that there was too much prompting, and then when they set the slider so it prompts less, they demand more prompting? Can these people make up their minds already?"

[1] Personally, it doesn't bother me. It's not like I spend my day constantly changing system settings. In fact, I keep my account out of the administrators group, so not only do I get prompted for everything, but when I do elevate to administrator, I'm running as the local administrator account, not as myself. This means that the elevated command prompt does not have domain network access (because domain access came from my domain account), and the domain account does not have administrator access.[2] This "separation of powers" helps limit the scope of any dumb mistakes I may make, since a rogue command running as administrator cannot access network resources, so any runaway command is limited to screwing up only my own machine.

[2] It's surprising how many programs stop working when faced with this dichotomy.

Raymond Chen

Follow