Welcome to MSDN Blogs Sign in | Join | Help

Engineering Windows 7

Welcome to our blog dedicated to the engineering of Microsoft Windows 7

Update on UAC

Hi, Jon DeVaan here to talk to you about the recent UAC feedback we've been receiving.

Most of our work finishing Windows 7 is focused on responding to feedback. The UAC feedback is interesting on a few dimensions of engineering decision making process. I thought that exploring those dimensions would make for an interesting e7 blog entry. This is our third discussion about UAC and for those interested in the evolution of the feature in Windows it is worth seeing the two previous posts (post #1 and post #2) and also reading the comments from many of you.

We are flattered by the response to the Windows 7 beta so far and working hard at further refining the product based on feedback and telemetry as we work towards the Release Candidate. For all of us working on Windows it is humbling to know that our work affects so many people around the world. The recent feedback is showing us just how much passion people have for Windows! Again we are humbled and excited to be a part of an amazing community of people working to bring the value of computing to a billion people around the world. Thank you very much for all of the thoughts and comments you have contributed so far.

UAC is one of those features that has a broad spectrum of viewpoints with advocates staking out both "ends" of the spectrum as well as all points in between, and often doing so rather stridently. In this case we might represent the ends of the spectrum as "security" on one end and "usability" on the other. Of course, this is not in reality a bi-polar issue. There is a spectrum of perfectly viable design points in between. Security experts around the world have lived with this basic tension forever, and there have certainly been systems designed to be so secure that they are secure from the people who are supposed to benefit from them. A personal example I have, is that my bank recently changed the security regimen on its online banking site. It is so convoluted I am switching banks. Seriously!

Clarifying Misperceptions

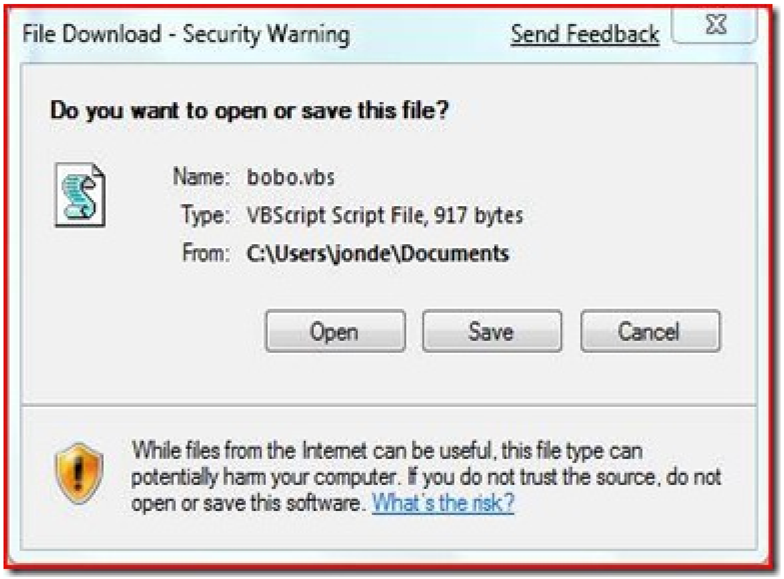
As people have commented on our current UAC design (and people have commented on those comments) it is clear that there is conflation of a few things, and a set of misperceptions that need to be cleared up before we talk about the engineering decisions made on UAC. These engineering decisions have been made while we carry forth our secure development lifecycle principles pioneered in Windows XP SP2, and most importantly the principle of "secure by default" as part of SD3+C. Windows 7 upholds those principles and does so with a renewed focus on making sure everyone feels they are in control of their PC experience as we have talked about in many posts.

The first issue to untangle is about the difference between malware making it onto a PC and being run, versus what it can do once it is running. There has been no report of a way for malware to make it onto a PC without consent. All of the feedback so far concerns the behavior of UAC once malware has found its way onto the PC and is running. Microsoft's position that the reports about UAC do not constitute a vulnerability is because the reports have not shown a way for malware to get onto the machine in the first place without express consent. Some people have taken the, "it's not a vulnerability" position to mean we aren't taking the other parts of the issue seriously. Please know we take all of the feedback we receive seriously.

The word "vulnerability" has a very specific meaning in the security area. Microsoft has one of the leading security agencies in the world in the Microsoft Security Response Center (secure@microsoft.com) which monitors the greater ecosystem for security threats and manages the response to any threat or vulnerability related to Microsoft products. By any definition that is

g
r
f

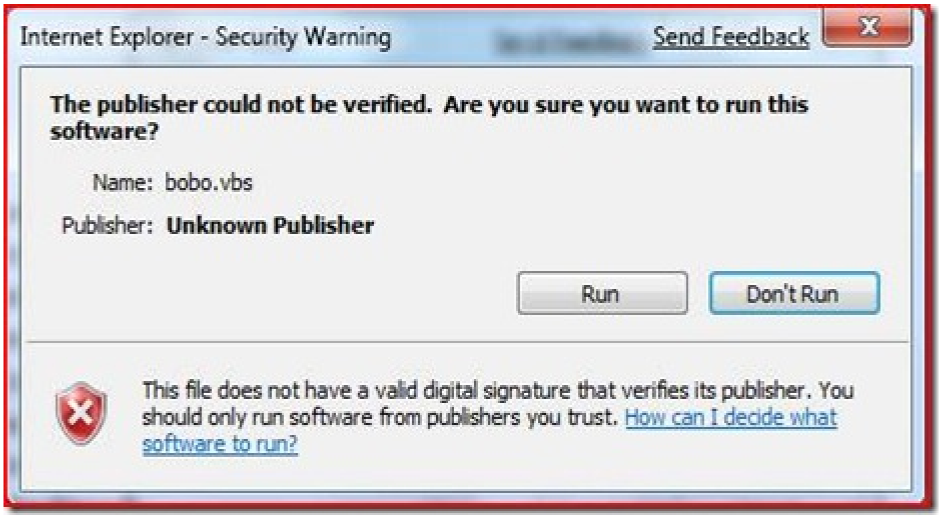
It is worth pointing out the defenses that exist in Windows Vista that keep malware from getting on the PC in the first place. In using Internet Explorer (other browsers have similar security steps as well) when attempting to browse to a .vbs file or .exe file, for example, the person will see the prompts below:


File Download - Security Warning

Do you want to open or save this file?

Name: bobo.vbs
Type: VBScript Script File, 917 bytes
From: C:\Users\jonde\Documents

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

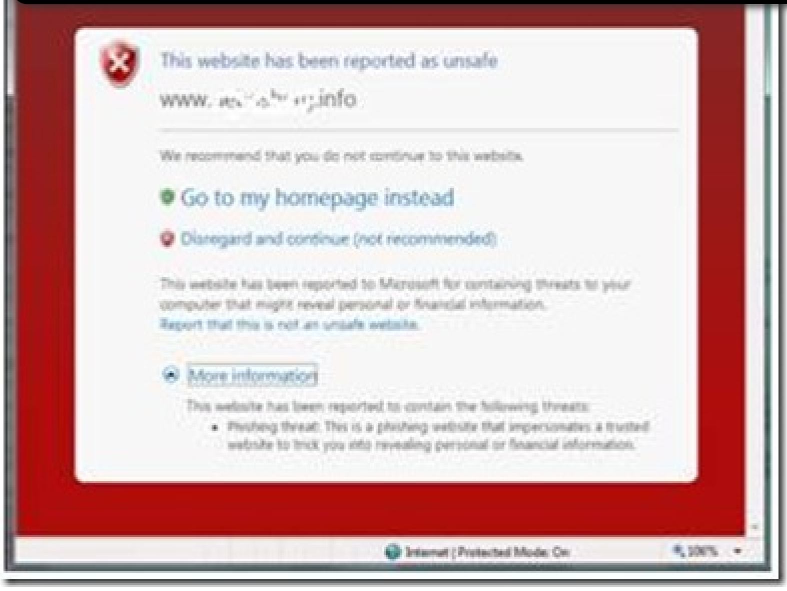

Internet Explorer - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: bobo.vbs
Publisher: **Unknown Publisher**

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Internet Explorer 8 has also introduced many new features to thwart malware distribution (see http://blogs.msdn.com/ie/archive/2008/08/29/trustworthy-browsing-with-ie8-summary.aspx). One of my favorites is the SmartScreen® Filter which helps people understand when they are about to visit a malicious site. There are other features visible and hidden that make getting malware onto a PC much more difficult.



This website has been reported as unsafe

www. [illegible].info

We recommend that you do not continue to this website.

Go to my homepage instead

Disregard and continue (not recommended)

This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.
Report that this is not an unsafe website.

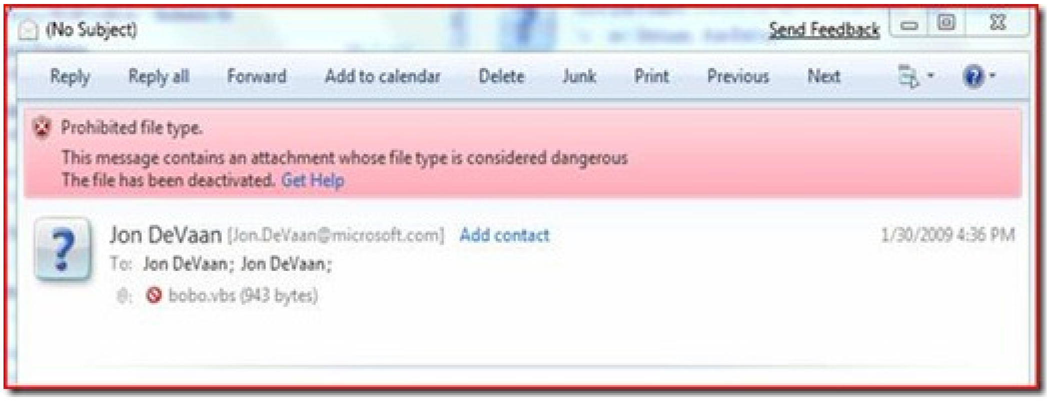
More information

This website has been reported to contain the following threats:

- Phishing threat: This is a phishing website that impersonates a trusted website to trick you into revealing personal or financial information.

A SmartScreen® display from IE 8

Additionally, if one attempts to open an attachment in a modern email program (such as Windows Live Mail) the malware file is blocked:



Prohibited file type.
This message contains an attachment whose file type is considered dangerous
The file has been deactivated. Get Help

Jon DeVaan [Jon.DeVaan@microsoft.com] Add contact 1/30/2009 4:36 PM
To: Jon DeVaan; Jon DeVaan;
bobo.vbs (943 bytes)

Much of the recent feedback has failed to take into account the ways that Windows 7 is better than Windows Vista at preventing malware from reaching the PC in the first place. In Windows 7 we have continued to focus on improving the ability to stop malware before it is installed or running on a PC.

The second issue to untangle is about the difference in behavior between different UAC settings. In Windows 7, we have four settings for the UAC feature: “Never Notify,” “Notify me only when programs try to make changes to my computer (without desktop dimming),” “Notify me only when programs try to make changes to my computer (with desktop dimming),” and “Always Notify.” In Windows Vista there were only two choices, the equivalent of “Never Notify” and “Always Notify.” The Vista UI made it difficult for people to choose “Never Notify” and thus choosing between extremes in the implementation. Windows 7 offers you more choice and control over this feature, which is particularly interesting to many of you based on the feedback we have received.

The recent feedback on UAC is about the behavior of the “Notify me only when programs try to make changes to my computer” settings. The feedback has been clear it is not related to UAC set to “Always Notify.” So if anyone says something like, “UAC is broken,” it is easy to see they are mischaracterizing the feedback.

The Purpose of UAC

Experience Improvement Program, Windows Feedback Panel, user surveys, user in field testing, and in house usability testing that the benefit of the information provided by the UAC consent dialog decreases substantially as the number of notifications increases. So for the general population, we know we have to present only key information to avoid the reflex to "answer yes".

One important thing to know is that UAC is not a security boundary. UAC helps people be more secure, but it is not a cure all. UAC helps most by being the prompt before software is installed. This part of UAC is in full force when the "Notify me only when…" setting is used. UAC also prompts for other system wide changes that require administrator privileges which, considered in the abstract, would seem to be an effective counter-measure to malware after it is running, but the practical experience is that its effect is limited. For example, clever malware will avoid operations that require elevation. There are other human behavior factors which were discussed in our earlier blog posts (post #1 and post #2).

UAC also helps software developers improve their programs to run without requiring administrator privileges. The most effective way to secure a system against malware is to run with standard user privileges. As more software works well without administrator privileges, more people will run as standard user. We expect that anyone responsible for a set of Windows 7 machines (such as IT Administrators or the family helpdesk worker (like me!)) will administer them to use standard user accounts. The recent feedback has noted explicitly that running as standard user works well. Administrators also have Group Policy at their disposal to enforce the UAC setting to "Always Notify" if they choose to manage their machines with administrator accounts instead of standard user accounts.

Recapping the discussion so far, we know that the recent feedback does not represent a security vulnerability because malicious software would already need to be running on the system. We know that Windows 7 and IE8 together provide improved protection for users to prevent malware from making it onto their machines. We know that the feedback does not apply to the "Always Notify" setting of UAC; and we know that UAC is not 100% effective at stopping malware once it is running. One might ask, why does the "Notify me only when…" setting exist, and why is it the default?

Customer-Driven Engineering

The creation of the "Notify me only when…" setting and our choice of it as the default is a design choice along the spectrum inherent in security design as mentioned above. Before we started Windows 7 we certainly had a lot of feedback about how the Vista UAC feature displayed too many prompts. The new UAC setting is designed to be responsive to this feedback. A lot of the recent feedback has been of the form of, "I'll set it to 'Always Notify,' but 'regular people' also need to be more secure." I am sure security conscious people feel that way, and I am glad that Windows 7 has the setting that works great for their needs. But what do these so called "regular people" want? How to choose the default, while honoring our secure design principles, for these people is a very interesting question.

In making our choice for the default setting for the Windows 7 beta we monitored the behavior of two groups of regular people running the M3 build. Half were set to "Notify me only when…" and half to "Always Notify." We analyzed the results and attitudes of these people to inform our choice. This study, along with our data from the Customer Experience Improvement Program, Windows Feedback Panel, user surveys, and in house usability testing, informed our choice for the beta, and informed the way we want to use telemetry from the beta to validate our final choice for the setting.

A key metric that came out of the study was the threshold of two prompts during a session. (A session is the time from power up to power down, or a day, whichever is shorter.) If people see more than two prompts in a session they feel that the prompts are irritating and interfering with their use of the computer. In comparing the two groups we found that the group with the "Always Notify" setting was nearly four times as likely to have sessions with more than two prompts (a 1 in 6.7 chance vs a 1 in 24 chance). We gathered the statistic for how many people in the sample had

We are very happy with the positive feedback we have received about UAC from beta testers and individual users overall. This helps us validate our "regular people" focus in terms of the trade-offs we continue to consider in this design choice. We will continue to monitor the feedback and our telemetry data to continue to improve our design choices on UAC.

So as you can see there is a lot of depth to the discussion of UAC and the improvements made in Windows 7 in UAC itself and in improving ways to prevent malware from ever reaching a PC. We are working hard to be responsive to the feedback we received from Vista to provide the right usability and security for people of all types. We believe we've made good progress and are listening carefully to the feedback on our UAC changes. Again please accept our most sincere thanks for the passion and feedback on Windows 7. While we cannot implement features the way each and every one of you might wish, we are listening and making a sincere effort to properly weigh all points of view. Our goal is to create a useful, useable, and secure Windows for all types of people.

Jon

Published Thursday, February 05, 2009 12:00 AM by e7blog
Filed under: E7Blog, Security, Design

Comments

# re: Update on UAC

I would like an option to keep expanded the Details shown in the UAC dialog box. Thanks

Thursday, February 05, 2009 5:11 AM by scalo

# re: Update on UAC

Would it be possible to add a simple check box, to allow the User to be notified if UAC level or setting was changed?

Thursday, February 05, 2009 6:12 AM by HappyAndyK

# It's about being reliable...

I think that the problem most people have isn't the default setting, but the fact that "Notify only when other applications..." doesn't actually work. Any application that is running can bypass this control and get as much access as if UAC wasn't running at all - not really a control is it?

UAC may not be technically considered a "security boundary", but in Vista, in practical use it was very close. In Vista if you run a malicious application, it can only affect your user account unless you specifically and explicitly allow it to do otherwise. Windows 7 makes that same promise, but doesn't deliver - that same malware, if adapted to 7, can take over the whole box. Performing the same set of actions in 7 shouldn't result in a worse outcome [than in Vista].

--

Aside from that I haven't actually met anyone who has complained about UAC... other than from what they have seen on an Apple ad. Most people so infrequently install apps, that it doesn't affect them. Maybe my case is weird they don't have any misbehaving legacy apps. UAC has improved the quality of Windows applications and Microsoft should be applauded for that.

If people want to take off their protection let them, but it's up to them to suffer the consequences.

If you can't make the default setting do what it say it does in a rock solid fashion, just use the known good Vista approach. (Just like every other OS on the planet)

Thursday, February 05, 2009 6:26 AM by fowl

# re: Update on UAC

session guideline (after all, you aren't going to be changing it often) but would prevent malware that has made it through the existing defences from changing the setting even lower.

Just because it isn't a security vulnerabilty doesn't mean that it's behaviour makes sense.

Thursday, February 05, 2009 6:30 AM by andycadley

# re: Update on UAC

While UAC may not be a security boundary, when the Operating System's default state allows any application to trivally have the System elevate arbitrary code, you no longer have a useful tool at all.

And the sources of malicious code are far more than that downloaded via Internet Explorer or an attachment-minding email client.

The long and the short of it is the token needed to adjust the UAC setting should be something above that granted by the autoElevate system.

Thursday, February 05, 2009 6:40 AM by hornetfig

# re: Update on UAC

Jon, you're missing the point. The people only want to see an UAC notification when the UAC level is changed. That's all.

You don't have to change anything else.

Thursday, February 05, 2009 8:00 AM by d_e

# re: Update on UAC

I'm not sure you only have to protect the UAC level. Does the default setting allow an application to do the following without any notification? ... only if Im an administrator or if Im a user?:

Replace a windows .dll

Uninstall a driver

Change services

Add executable to startup

... etc

Assuming an app could do all of this silently, what good is UAC for at this point anyway. Why not just remove it.

-d

Thursday, February 05, 2009 8:18 AM by dugbug

# re: Update on UAC

While I understand that you do not consider UAC the ultimate barrier against malware, even with all the new security barriers in mail, IM and IE8 you saw that it did not prevent for malware to be installed.

So, a new barrier should be running to prevent the installed malware to harm the computer.

Naturally, this barrier can be the UAC (although I'm pretty sure a lot of malware can run in user mode if its just collecting data..)

Thursday, February 05, 2009 8:20 AM by ups

# re: Update on UAC

with all those REQUEST , become 40 SKU of Windows 7 :D

Thursday, February 05, 2009 8:34 AM by Domenico don't want to remove or change the way auto-elevation works.

Thursday, February 05, 2009 8:38 AM by tryon

# re: Update on UAC

Look at it this way - let's say I let my son bring a friend over, even one who I thought was trustworthy.

I dont need to be notified if he takes a drink from my fridge or sits on my chair. But I'd REALLY like to be notified if he's trying to remove the locks to my bedroom door.

The changing of the UAC setting itself must be an exception. It is a fundamentally different setting than any other setting. I simply dont understand how this is not painfully obvious. If not for the reality of this situation, then for the perception. If you guys are correct, the only people that should see this are people already infected with malware, so a second reminder that something really fishy is going on is not going to hurt.

Thursday, February 05, 2009 8:40 AM by mdaria510

# re: Update on UAC

Wow. Wrong answer.

The Microsoft response to this issue is really shaking my faith the quality of Windows 7. Vista was full of the sort of obtuse thinking. Every single person outside of Microsoft knows the fix for this, its mentioned multiple times in the comment in this thread.

Put on your "common sense" hat and just fix the issue, guys. It's not that difficult.

Thursday, February 05, 2009 8:53 AM by mech9t8

# re: Update on UAC

I think part of the issue here is the fact that there is an assumption that any untoward goings on will only ever be caused by malware or spyware.

As far as Im concerned, no application trusted or otherwise, should be able to alter the core UAC settings without express permission from the user (via a UAC prompt). As it currently is in the beta, any application running on the system can very easily and silently disable UAC completely, thereby giving itself and any other app that wants it, full access to the system. That alone completely nullifies the point of having UAC or any other security boundary in the first place, if it can be so easily tampered with by any running process.

I do agree with Microsoft's assertion that UAC was not specifically designed as a fool proof security barrier, but it is however an important part of Windows' security model and should be treated as such. As it currently is in the beta, it can be so easily disabled it may as well not be there at all. As others have pointed out, the default setting is fine (And works well) but there certainly needs to be some kind of prompt when attempting to change UAC's core settings.

Thursday, February 05, 2009 8:55 AM by phobox

# re: Update on UAC

Sometimes, inconsistency with your own ideals is a good thing. Make an exception, if only to put people's fears to rest.

Thursday, February 05, 2009 8:57 AM by mdaria510

# re: Update on UAC

I see your point that the malware *should* never get onto the computer in the first place, but imagine if I downloaded a piece of software that unknown to me had malware piggybacking on it. I would click through the UAC promts thinking I was installing a legit program, while in the background this program is also being installed. Rafael Rivera's list of EXE's that can be evelevated without

HUGE! The list of allowed programs could be managed in the control panel.

Anyway, thanks for all your work on UAC!

Thursday, February 05, 2009 9:05 AM by RyGuy12

# re: Update on UAC

Jon, let me quote poster above, just in case you missed it:

"

Jon, you're missing the point. The people only want to see an UAC notification when the UAC level is changed. That's all.

You don't have to change anything else.

"

Please stop giving *@*! excuses. It is not working as expected. Surely if I run vbs script I don't expect it to be able to completely turn off UAC. Let me know if it tries to change my UAC settings. That is all.

Thanks.

Thursday, February 05, 2009 9:10 AM by adamc60

# re: Update on UAC

Don't deal with treat UAC settings like Windows settings, this would cause UAC prompt when people change UAC settings, would be a perfect solution in my opinion.

In this situation there are no reductions in security and usability.

Thursday, February 05, 2009 9:12 AM by sirus

# re: Update on UAC

Think of it like the security/ID badges you use at work. If you are authorized to enter a certain area, this is reflected by your badge and you walk right in. If you are not, then you must show some documentation granting permission.

This would be a UAC prompt.

If the change is to be made permanent and you are given full access you would still expect to the change to be validated before being granted access.

This is a UAC prompt for UAC changes.

Why should it be easier to get permanent access to a controlled resource than to get temporary access? Sure, no one in the company SHOULD be asking for access if they are not supposed to have it, but that doesn't mean they won't.

Why should it be easier to turn off UAC than to act maliciously with UAC? Sure, no malware SHOULD be running on the PC, but that doesn't mean it won't.

1 additional prompt that very few people will ever see and it greatly increases the faith people have in this whole system. If I know that changes needing elevation will be prompted and I don't see any prompts, I feel fine. If I know that at any time, UAC prompts could be disabled without prompting, then I would immediately turn it up to full and live with the extra hassle.

I rarely ever leave comments anywhere. In fact I had to register just to leave this comment, but I feel strongly enough about this issue that it definitely warrants attention.

Thursday, February 05, 2009 9:49 AM by Jaquez

# re: Update on UAC

matter how great you make IE, there will still be a significant portion of W7 users who prefer an alternative browser. You CANNOT make assumptions on security of the OS based on the behaviors on IE8.

Here's a few ideas, from my experiences with Vista's UAC, how people react to it and why they turn it off:

1. The initial installation period when you are installing your applications leaves a false bad impression of how many times UAC will be bugging users. What needs to happen here is the implementation of an "install mode" for UAC - a prompt when the first piece of software is installed that allows the users to turn off UAC for the remainder of the current session with a warning to not access potentially unsafe locations or files while this mode is active, along with a CLEAR notification to the user that they are in this mode - perhaps changing the desktop theme to a special one while the mode is active. On the next reboot, a greyed screen UAC prompt will ask them if they are done installing applications, and offering them a yes or no prompt; a yes puts the computer back into normal non- auto-elevate mode, a no leaves install mode active.

Second, change the implementation of the "always run as administrator" checkbox so that it auto-elevates the application in question and runs it without a prompt. It's just plain silly for me to have to approve an app that I have already auto-approved every time I start it - especially when I had to go through UAC elevation just to check the box!

Last, allow application designers to prompt the user with an auto-elevation prompt on install; this would simply check the "run as admin" checkbox, as implemented above. This would allow applications that always need to run elevated to do so without the user having to be smart enough to go in and check the box themselves (MMO games that auto-update themselves spring to mind).

I hope you take these suggestions to heart, they're a much better alternative to just allowing apps to elevate themselves and relying on the user to use data access sources that you have control over.

Thursday, February 05, 2009 9:57 AM by jturnley

# re: Update on UAC

I really like UAC. No, wrong, I LOVE UAC.

And John, you are right in all points and it everything you say is correct.

However most people are worried about the issue mentioned here: http://www.istartedsomething.com/20090130/uac-security-flaw-windows-7-beta-proof/

So I'd like to provide a little different view and ask: Why do you force people to enter the old password when changing it? In fact they already had to enter the password when logging on to their PC so why bother with it again?

Answer: Because it's more secure.

Why not take the same route with UAC and always ask about elevation when the elevation settings are changed? Even if it wouldn't be more secure (according to your studies) people would at least FEEL more secure - and that is most important for technical folks.

Kind regards,

Ooh

Thursday, February 05, 2009 10:04 AM by Ooh

# re: Update on UAC

> "The people only want to see an UAC

> notification when the UAC level is

evil setup program has no need to disable UAC. If it decides to do so, it would most likely change the registry setting directly rather than go to the trouble of pushing keystrokes into the UI the way Long Zheng's "exploit" did.

So can anyone explain a scenario where this one extra annoy-o-gram ("You are attempting to change the UAC setting via the Windows dialog, please confirm") is going to have any real effect?

Thursday, February 05, 2009 10:38 AM by StubToe

# re: Update on UAC

It's obvious MS still doesn't take this issue seriously. Hell, they don't even consider UAC to be a security boundary. I'm just gonna go back to Vista so I can at least feel safe and confident that UAC will work as it should. If these UAC issues aren't resolved by RTM, I simply won't be upgrading to 7 and I won't be recommending it to anyone.

The biggest mistake was bending to the will of idiots who simply do not understand UAC, so now we get this inconsistent behavior about UAC by default.

Thursday, February 05, 2009 10:48 AM by xiphi

# re: Update on UAC

#1-

The simple solution is to pop-up a UAC prompt *regardless of its current setting* whenever the UAC level is modified. The only time you'd expect to see such a prompt is when you just finished making a change to UAC preferences. If you saw it any other time, it would clearly be malware.

I see where Microsoft is coming from - the lower level by design doesn't prompt for Windows settings. However, UAC should be an exception.

#2- If they want people to run as reduced-privilege accounts, OFFER to set one up during installation. Most people don't go out of their way to give themselves fewer privileges, but if you explain the merits of it during install and let them optionally set up a 2nd username/password, chances are increased. My XP runs as power user but nearly everyone else's XP runs as administrator.

#3- Elevation prompts are a reality of any OS, OSX and Linux both prompt you to elevate privileges, albeit with a password prompt instead of a yes/no box. Apple's silly ad was a little unfair there, it appeared more often in Vista because everyone was running software written in an era where nearly everyone's Windows account was an administrator.

Thursday, February 05, 2009 11:13 AM by bananaman

# re: Update on UAC

@StubToe

It's the exploited Outlook scenario. Imagine a bug in Outlook allows arbitrary code execution:

* On Vista, that code can't get elevated permissions without a UAC prompt.

* On Windows 7 (as is) it can disable UAC and then elevate silently.

* On Windows 7 (if it took a UAC prompt to disable UAC) you'd be in the same situation as Vista.

Of course, if you agree to the UAC prompt, then anything can happen in either case. But that isn't the scenario UAC provides protection for and it never was.

Thursday, February 05, 2009 11:18 AM by andycadley

# re: Update on UAC

One final thought- Microsoft should fix this "problem" even if not considered a vulnerability, if for no other reason than to get Win 7 off on the right foot. After Vista they could use some good press and

@xiphi: UAC can be configured on Windows 7 to behave exactly as it does on Vista. You only have that problem with the default configuration.

@Ooh: I agree with you. Although I can see the point MS is making, now it's a matter of perceived security (and bad press).

Thursday, February 05, 2009 11:44 AM by guillermo.vega

# Defence in depth?

Wouldn't a simple and transparent fix be to run control panel windows (like the UAC change window) at a high integrity level automatically? Then there would be risk of the control panel being hijacked at all.

As it stands I just can't understand the logic that says 'this isn't a problem'. UAC could get annoying in Vista sometimes, but it was worthwhile regardless because it provided some tangible benefit. The default setting in Windows 7 is just pointless! Why bother having an annoying elevation dialog which only applies to well behaved software? When Vista came out the philosophy was defence in depth. How quickly we forget.

Thursday, February 05, 2009 11:52 AM by jepzilla

# re: Update on UAC

My conspiracy theory is that Microsoft disabled UAC by default in Windows 7 to raise this very discussion which even got its way into printed press. Their goal is to make us ask to have UAC in “Always Notify” mode in RTM. And I do ask that because people I know don’t have any issues with Vista UAC because they only use Internet Explorer and Microsoft Word.

When I first heard about UAC changes what I hoped for was more granular control over changes. I mean why you need UAC to change DPI? What kind of malware might want to change DPI? And that was changed in Windows 7. There is no UAC prompt to change DPI in Windows 7.

Here we have another thing which is to allow specially signed executables to change critical settings without UAC prompt.

Here is interesting thing. With UAC in “notify only when programs try…” mode I am still presented with UAC prompt when I try to run regedit.exe (WHY??). But if I go and disable UAC at all – which is allowed without any prompt I immediately can go and run regedit.exe without any UAC Prompt.

If MS does not allow running regedit.exe in “broken-UAC” mode why does it allow switching UAC mode off?

This all seems very inconsistent. I have switched to “always notify” mode.

Thursday, February 05, 2009 12:17 PM by Vyacheslav Lanovets

# re: Update on UAC

After your explanation I think SEVEN = Software Enviroment Vulnerable Exploitable Nackered. Why UAC at this point anyway. Why not just remove it Microsoft.

The joke today on internet is sponsored by Microsoft Windows 7 UAC Team: The Windows 7 shirts have four holes on them, but the manufacturer has been assured that it is by design. So is better distribute condoms because have only one hole and is more secure against virus and infections by design.

Thursday, February 05, 2009 12:39 PM by E-ponto

# re: Update on UAC

The fact Jon is missing is a malware can 'become' any application written in what is technically known as memory-unsafe (or type-unsafe) computer language like highly popular C or C++. These two languages are still widely used by Microsoft and other developers. The problem with such

(http://en.wikipedia.org/wiki/Buffer_overflow)

With this in mind we can see that every program written in said languages can never be trusted completely, we can be never completely sure the program is free of errors and because of this every program can start acting as 'malware'. Microsoft Office, most of Windows, IIS and Internet Explorer are written in C(++) and are historically known to be vulnerable to attacks that use errors I described above. While it is hard to believe MS Word would ever act as malware, but if feed the right input (example would be a file user received through email) the program will make an error and because the input was specially crafted beforehand the Word will get reprogrammed to act as malware, maybe it will even resend document to other people and act as a worm.

This is not science fiction; it is real world problem that security experts have to deal with. The fact that every application can act as malware is in contrast to Jon's belief that file/binary with virulent content has to be present on user's disk for user to get infected.

The problem is that when program is running in default/'Medium IL' mode of UAC in Vista a program is not able to control the system. In Windows 7 with default UAC setting however a program in 'Medium IL' can circumvent the protection, disable UAC altogether and start running 'High IL' mode - all this automatically without the need for user to confirm anything. While Vista would stop and display UAC dialog in Windows 7, a malicious code can just walk away and help itself.

This is not frightening only because there is by default no boundary between 'Medium IL' and 'High IL', but also because the user is misled by a belief that he is running in 'secure mode' because every program that did not come with Windows, has not yet been compromised and is running in 'Medium IL' will display UAC window when it will require administrative privileges ('High IL').

Because applications will still display UAC dialogs user will think he is safe, but because UAC can be currently easily avoided user is not really safe - the way UAC works now is highly ambiguous.

Now I'll go to what I think the team responsible for security in Windows 7 had in mind when they implemented the new model.

Because many applications that come with windows cannot receive input originating from other than the user himself Windows will allow it to make administrative tasks without UAC dialogs. Windows Explorer and Control Panel for example do not open documents, neither do they access internet and thus have a small attack surface meaning it's highly unlikely anyone can compromise them and so it's safe to automatically run them in 'High IL' mode. On the other hand Internet Explorer has a huge attack vector and has been thus running in 'Low IL' since Vista.

I have to agree that this model is neat, it will remove a lot of UAC dialogs when working with Windows and will be secure - the only problem is the bug bloggers described - it can be easily fixed by disallowing any messages that originate in 'Medium IL' and are moving towards 'High IL' - just like 'Low IL' cannot talk to 'Medium IL' currently.

I should also mention that if this bug does not get fixed Windows 7 will fall back into XP model of 'full admin by default'. In recent news a company claimed that more than 90 % of vulnerabilities could be prevented if users did not run in Admin mode. If this bug stays it means Windows 7 will see more worms than Vista had.

(http://www.computerworld.com/action/article.do?command=viewarticlebasic&articleid=9127318)

If the bug stays then Microsoft will indeed see less negative responses from those that think UAC is annoying, but I expect much much bigger backlash from bloggers for relaxing security.

I'm writing this response to this UAC fiasco only after many MS employees (some in very high positions) tried to deny the existence of the bug. I firmly believe the team responsible security is aware of the bug, it just bothers me to see people so high in the management hierarchy talk about something they know in details - it is not good promotion for a company and it really reduces confidence in the competence of people inside. The security of a system is not something you can

Thursday, February 05, 2009 12:56 PM by RoyalSchrubber

# Please listen to us

Jon,

Thanks for sharing your thoughts. I understand your points.

Now, I want add my voice to the call for one very simple change:

Treat the UAC prompting level as a special case, such that ANY change to it, whether from the user or a program, generates a UAC prompt, regardless of the type of account the user has, and regardless of the current prompting level.

That is all we are asking. No other changes. Leave the default level as it is, and keep UAC as it is. We're just talking about the very specific case of CHANGES to the UAC prompting level.

It will NOT be a big nuisance - most people only ever change the UAC level once (if at all).

Despite your assurances, I REALLY WANT TO KNOW if anything tries to alter the UAC prompting level.

The fact that nobody has yet demonstrated how the putative malware can get into your machine is NO argument. Somebody WILL get past those other boundaries eventually.

Even if you aren't convinced by my argument, then the PR argument must be a no-brainer for Microsoft.

PLEASE, Jon, it's just a small change that will gain a LOT of user confidence and a LOT of good PR.

Thack

Thursday, February 05, 2009 12:58 PM by Thack

# re: Update on UAC

I definitly agree with the idea to add an option when installing windows to create both a local admin account as well as a standard-user account. That would be a *huge* help in encouraging the use of standard-user accounts.

I also agree that even if you guys don't think it's a big issue, there are lots of people in the real world that do. You keep saying you listen to your customers, listen to us and at least add a prompt when changing the UAC notification level.

Thursday, February 05, 2009 1:04 PM by mesan

# re: Update on UAC

I don't get this mind-boggling, the-customer-is-stupid response! If 7 can keep malware off of the computer, what is the point of UAC at all that I, as an individual customer, care about?

Look, just fix this little issue. Laugh at me behind my back, send little sarcastic emails amongst yourselves, I don't care, just don't force my to set UAC to "Always Notify", please.

I'll sleep better at night.

Thursday, February 05, 2009 1:12 PM by joe7pak

# Unauthorized code does happen

Quote: "The first issue to untangle is about the difference between malware making it onto a PC and being run, versus what it can do once it is running. There has been no report of a way for malware to make it onto a PC without consent."

I find that statement inconsistent with the Microsoft Security Intelligence Report (http://www.microsoft.com/sir), which has statistics showing ways that malware does make it onto

t
F
e

I've run into such exploits myself. Protected Mode took care of them, since I use Internet Explorer. But if the user is running a browser without Protected Mode, that mitigation will not help them. And if they're running as an Administrator, as Windows set their first user account up by default, what will happen?

For another real-world example, F-Secure's blog shows the clever ruse used by Conficker.B to get people to execute the infection when they think they're just opening Explorer to view the contents of a USB drive:

http://www.f-secure.com/weblog/archives/00001586.html

In my opinion, considering the ingenuity and determination the bad guys have shown over the last decade, it is naive to think that there will be no non-user-initiated malicious code execution on ~500 million PCs from 2010 to 2021. Put up walls around the UAC settings, at a minimum. I also suggest using the secure desktop by default; people *are* getting accustomed to UAC, especially since Vista SP1.

Thursday, February 05, 2009 1:43 PM by mechBgon

# re: Update on UAC

Am I missing something. Could Microsoft not setup mechanism to allow only an authorized subsystem to change the UAC settings or disable it altogther. ie digitially signed

Thursday, February 05, 2009 1:50 PM by kevin.weir

# re: Update on UAC

You have 95% of the people out there think you got it wrong, even if they are the ones that got it wrong. The problem is that they are the one's that buy and recommend your product. So do you give them a false sense of increased security by implementing the change (not unlike security by obscurity) and making them happy, or do you just fortify the real security boundaries?

Personally, I think you make people happy and sell product. Though acknowledge that you will suddenly have lots of similar items in the same class of "I installed something and it is doing something I didn't think it would do".

The general public understands and appreciates security by obscurity (they still hide things under the mattress, or someplace hidden in their house), even though the security industry thinks it is bad since it brings a false sense of security that they do not have. But people relate to it anyhow.

Doesn't sound like an engineering decision. Sounds like a business one.

Thursday, February 05, 2009 2:30 PM by sroussey

# re: Update on UAC

I'm not sure I get it. Why exactly are you championing limited user accounts again? Going by what you said, once a piece of software gets on the PC, it doesn't matter what it does, it won't be a security vulnerability.

Why is there limited access rights to some files on the OS? Why can't my application change security-related settings without sufficient privileges?

Going by this blog post, none of that would be necessary, because "there's no way for software which exploits it to get onto the PC".

And yet all those features were there in Vista, and are there in Win7.

It does seem weird that a program running without superuser privileges, is able to disable UAC without prompting the user.

In the default setting, UAC requires confirmation for security-related changes, but ignores everything else. Why exactly is UAC's configuration itself not a security setting?

is needed", then it begs the question "why exactly is UAC there, then?"

It seems you're intent on nitpicking about the precise definition of malware, and are assuming a perfect world with no security vulnerabilities in the browser, and an omniscient user who would never execute a piece of malware in the first place.

And that just misses the point that users aren't perfect, malware *will* end up on the machine, and if the user can't trust UAC to warn them if it attempts to perform critical security changes, the UAC becomes pretty useless.

Considering how badly behaved most Windows software is, isn't it naive to assume that "malware is something that will give the user a warning when he downloads it"?

What exactly are the odds that some software developers will choose the lazy way to "fix" the UAC prompts their (otherwise benign) software causes? I'm willing to be that some of them will simply decide "eh, we'll just lower the UAC setting a bit. The user won't notice the difference, and it means I won't annoy him with UAC prompts all the time".

Thursday, February 05, 2009 3:19 PM by Jalf

# re: Update on UAC

Jon,

this is unbelievable. Such a long blog entry and you never come to the point. How long do you want to hide behind telemetry data? This is not a way to communicate with smart people.

You are either dumb (don't think so) or you make yourself look like dumb because you have actually seen through this.

First the question of how malware comes to run on the computer is completely irrelevant for this, because UAC prompts are about programs which already run on the computer.

One question really raised here is if the UAC prompt is special for UAC or not. Maybe you think it is not special and have a good reason for that. But I can't imagine that a smart guy did not see this question asked here.

So I think what you do not tell us here is that you fear if you give in in this case and put an UAC prompt before UAC changes, people will come up with further cases where programs bypass UAC by simulating user input rendering the whole concept of the new default setting useless. But then maybe it is useless.

Obviously this would be hard for you to swallow at this point. But you have more to lose by not having an honest discussion.

Thursday, February 05, 2009 3:25 PM by Mikael3

# re: Update on UAC

I think a clarification on whether UAC can be changed programmatically and whether there will always be a UAC prompt if this happens would help here... but the figures on usage and malware incidence from the M3 are very interesting. Do you consider the M3 user base representative of the general user base or might there be a skew towards more 'careful' users? I'm assuming you'll look at the same figures from beta users and evaluate that...

Thursday, February 05, 2009 3:27 PM by marypcb

# re: Update on UAC

As many said before me: Changing UAC Prompting Level should trigger an UAC prompt!

Thursday, February 05, 2009 4:03 PM by Joop

# re: Update on UAC

S
F
I
my doors...

Just doesn't make any sense. What am I missing?

Thursday, February 05, 2009 4:07 PM by Ian Morley

# re: Update on UAC

I can't see that having a UAC prompt if something attempts to change UAC itself would be a bad thing. I would rather know if something has just changed the security level I have elected!!

Slightly off topic, I have just read that it has been confirmed that ther will be 6 versions of Windows 7.

http://www.pcpro.co.uk/blogs/2009/02/03/making-sense-of-microsoft/

PLEASE REVERSE THIS DECISION!!!!

You only need Home and Business in the mainstream, anything else just causes confusion. If you want to have a host of other versions for big corporates that's fine, just don't release them or even mention them to the general public.

I waste so much of my day explaining the stupid versions of Vista to worried customers. At the end they only ever want a home version or a work version.

Just sell the home one at a really keen price £50 in the UK which is probably $50 in the US, sell the Business version for £/$80 and you will absolutely rake it in.

Sell the OEM versions of the above for £40 and $60 and MS profits will go ballistic!

There are so many XP users dying to ditch it for a modern OS and this is your big chance.

Do anything else and you will see Ubuntu and OSX ripping into your market share.

I do not believe it ... 6 versions, do the marketing drones not learn anything, we are in a recession both sides of the pond.

If I was a coder in Redmond I would take industrial action against this decision. All the brilliant work being done by the guys and gals who report here is being thrown away!!

Siv

Thursday, February 05, 2009 4:10 PM by dotnet@sivill.com

# To add to what marypcb said...

...let's touch on this quote from the blog here:

quote: "In making our choice for the default setting for the Windows 7 beta we monitored the behavior of two groups of regular people running the M3 build. Half were set to “Notify me only when…” and half to “Always Notify.” We analyzed the results and attitudes of these people to inform our choice. This study, along with our data from the Customer Experience Improvement Program, Windows Feedback Panel, user surveys, and in house usability testing, informed our choice for the beta, and informed the way we want to use telemetry from the beta to validate our final choice for the setting."

I've hunted malware in the real world. At one point, I was turning in more malware samples in an average day than the entire CastleCops MIRT. After sneaking thousands upon thousands of malware samples past Defender without detection, I can safely say that Windows Defender's ability to detect fresh real-world malware is distressingly low. I cannot accept your Defender detection statistics as a meaningful metric here.

I would also like to point out that the test you've describe is merely testing for today's security landscape, not for the next ten years. It's wise to plan for the future, not for the past, because once notification, so that the Security Center could not alert users that their antivirus software had been turned off to pave the way for further infections.

The bad guys frequently molest other Windows features as well. For example: System Restore points are destroyed to prevent an easy recovery. The Windows Firewall is disabled, or exceptions are added. Browser security settings are altered. DEPEND ON IT: if you leave these controls accessible to userland code on a default out-of-the-box Windows installation, the bad guys will not ignore them in the interest of "fighting fair."

Those who do not know their history, are doomed to repeat it...

Thursday, February 05, 2009 4:10 PM by mechBgon

# re: Update on UAC

I read through your blog once again and there is in fact a single sentence, which really comes to the point of this discussion. The sentence is:

"For example, clever malware will avoid operations that require elevation."

It seems to me that you talk about UAC in general here including the strong version, which is currently active in vista.

Can you please elaborate on how malware would do that. Is it then true that the only purpose of UAC is to torture end users to force programmers change their programs? If this is not a security feature, then why lock the desktop for an UAC prompt?

I also do not understand this sentence:

"UAC helps most by being the prompt before software is installed. This part of UAC is in full force when the "Notify me only when…" setting is used."

Can you please elaborate.

Thursday, February 05, 2009 4:14 PM by Mikael3

# re: Update on UAC

Well, I hope you already got the picture by the many comments. I think your reasons and your logic are faulty. With security as a high priority, this should be a no brainer. I think you should ALWAYS UAC prompt for changes to UAC. If you do not want to do that, then you should always prompt for UAC if the change is going to be set to a lower value than the current setting. This is more work I am sure but I think that is the minimum bar. The better solution, is to just always prompt for changes to UAC. I can kind-of see not prompting for UAC if UAC prompt is disabled completely but that is the only scenario that I would accept as valid for not prompting.

Thursday, February 05, 2009 4:18 PM by DanStolts

# re: Update on UAC

I feel that Windows or Setup does not encourage users enough to run as normal user.

Most users that are mostly the only users of their computer create only 1 user account and that becomes the account with admin rights.

Setup should be changed in a way that it becomes normal for any computer user that a normal user account is created that will be used normally, and that the admin account is only used for very specific scenario's.

Thursday, February 05, 2009 4:23 PM by davidvl

# The problem is not solved by just adding a prompt for UAC changes!

What most people seem to forget when they ask for an additional UAC prompt is that this DOES NOT solve the problem AT ALL!

A
b
e

Example: If malware wants to copy itself into the Windows system folder or change any system files, it can do so by simulating user interaction with Explorer. This is because in the default Windows 7 UAC setting you wont get prompted if you use Explorer to make any changes to system folders.

Why is this not considered a security problem?!

As already said: The OS cannot base its security on the assumption that there are external mechanisms to prevent malware from getting onto the system. Instead this is where OS security comes in. Its the OS's job to prevent that running malware damages the system.

Perhaps the problem could be solved by using integrity levels. Raise the integrity level of the applications/dialogs you want to be allowed for auto-elevation above medium (somewhere between medium and high) and deny medium-IL applications the communication (sending keystrokes etc.) with higher-IL applications/dialogs.

Thursday, February 05, 2009 4:47 PM by hux

# re: Update on UAC

I think the big unword in this article is "Customer-Driven Engineering".

Customers will always ask for more gummi bears. But if they get problems with their stomach, then it is of course the fault of the engineer.

Thursday, February 05, 2009 4:49 PM by Mikael3

# re: Update on UAC

@hux

I think your point explains the reaction of Microsoft to this. The new UAC level seems to be fundamentally flawed, so it becomes difficult to draw a line for them.

But then doesn't it make a difference for practical security, if a malware script has to just switch off UAC or simulate lengthy user explorer sessions. These are the kind of considerations, I expected from Jon's blog and not pointless telemetry data.

Thursday, February 05, 2009 5:00 PM by Mikael3

# re: Update on UAC

I would suggest the Microsoft security group work with the Comodo team on how to properly display a popup, how to display the information (have a Basic and an Advanced option), AND how to properly implement a firewall. The XP, Vista and W7 firewalls are so useless that any script kiddie with more than 10 minutes can be into the OS (direct broadband connection, no NAT firewall, no software firewall aside of default Windows Firewall). UAC is only useful for the clueless customer that wants that warm fuzzy feeling of "thinking" that they are safe with UAC on.

Thursday, February 05, 2009 5:07 PM by screwballl

# Re: Defender detection rates as a metric

Previously, I mentioned that Defender's detection rates aren't too great. As an illustration, I pulled 2236 malware samples out of my archives, and scanned them with Defender, as well as with Kaspersky's online scanner.

Here are screenshots showing the results (namely, Defender detects 95 of the 2236 samples, while Kaspersky detects 2216 of them).

http://i240.photobucket.com/albums/ff237/mechBgon/Defender.png

http://i240.photobucket.com/albums/ff237/mechBgon/Kaspersky.png

Keep in mind that these samples are more than a year old. I hope the Win7 team is also using other software, such as OneCare or another full antivirus program, to generate metrics on infection rates.

Instead I would like to see sime kind of "don't warn me for the next 30 minutes" option in the UAC screen.

Also I would like to have special UAC mode in which it is allowed to do different not very harmful things like list running processes from All Users in Task Manager, launch chkdsk.exe or defrag, even connect or disconnect from network.

But replacing system files in Windows Explorer, updating device driver, change security permissions - all these should be UAC protected.

Thursday, February 05, 2009 5:15 PM by Vyacheslav Lanovets

# re: Update on UAC

Great explanation on UAC and how MS puts so much faith in the very narrow & limited user groups and surveys, instead of relying on 'real' users in the field as represented mainly by their many beta testers who DO represent and deal with the 'ordinary users' every day.

This blog post, while eloquently presented, says one thing mainly: 'that MS, again, can't see the forest for the trees'. :)

Thursday, February 05, 2009 5:26 PM by artfudd

# re: Update on UAC

@Mikael3

You are right. The new UAC level is definitely flawed and they have a deeper design problem here that is not fixed by just adding a single prompt. If they were to add a prompt for UAC changes then someone would come along and do a quick demo on "How to turn of the W7 firewall without UAC prompting for elevation".

They really have to reconsider the current implementation of the new UAC level and I think (as mentioned earlier) a more extensive use of integrity levels could possibly do the job here.

It would be interesting to see Jon commenting on such ideas.

Thursday, February 05, 2009 5:27 PM by hux

# re: Update on UAC

I'd accept that this is quite a valid argument. UAC can only protect you so much, but the onus is on your part to not click yes to run anything, but that also leads to one issue, where people can further circumvent this and make things seem more legit, and that is through an MSI installer, just imagine applications bundled with the reg key. I mean elevating for an MSI installer is pretty common, and if the malware vendor or what not, is intending to try to give away free software and also in turn getting the user to elevate the install so that they can install the reg key, then it's really not the users fault to unknowingly allowing elevation, as the installer could be well packaged really nicely and the app could very well be an excellent app, giving good incentives to the user.

Thursday, February 05, 2009 5:37 PM by winstonpang@hotmail.com

# re: Update on UAC

@Vyacheslav

Turning UAC off for 30 minutes is the same as turning it off altogether; how do you know those aren't the 30 minutes when you'll be hit by malware? And the things you list as 'not harmful' will usually have a good reason for needing to run as admin; malware would love to elevate and see what system processes it can attack.

@Siv - and I know I shouldn't perpetuate an off-topic discussion, but despite the list of 6 SKUs, your customers will only see 2/3 of them: the home version and the business version on the shelf, and the version with the extras on a high-end gaming machine that they can also choose to upgrade to online

Thursday, February 05, 2009 5:43 PM by marypcb

# re: Update on UAC

Is no one else surprised that malware can change UAC settings? There should be absolutely no method for applications to change UAC settings in the first place. And users should always be prompted for decreasing UAC settings, the above example of someone letting their child use their PC is a good reason why this should be the case. Sure, malware has to be prompted to allow these things to run, but, at least in Vista, when the malware is removed UAC is still there at the end of the day. On 7, once it's disabled it will probably remain that way for a while as users aren't likely to re-enable a feature that "nags" or "second-guesses" them.

By-the-by, this post sure has gotten a lot of responses quickly. The nerds are angry! :-)

Thursday, February 05, 2009 5:56 PM by Vistaline

# Please explain why UAC shouldn't protect itself

I really see no reason why attempting to change the UAC setting (unless it is turned off) shouldn't trigger a UAC prompt... I understand the customer feedback around UAC, but c'mon--that feedback is hardly relevant to changing the UAC setting itself!

I realize this analogy isn't perfect, but a lock on your door really isn't very effective if the thief can simply remove the lock itself by removing a single screw. Yes, it's true that it appears that a UAC-disabling exploit may already mean "game over" for that machine, but consider this: that's hardly *always* true, and even then, isn't it better to continue to protect the machine against further infection, particularly against many, many older malwares that would have otherwise been rendered ineffective by UAC? And isn't it better for the state of the UAC setting to be a potential wildcard?

I think the real question here is why *shouldn't* UAC protect itself, and that hasn't been answered here. I see no reason.

Thursday, February 05, 2009 6:01 PM by bluvg

# Again: A prompt at UAC level change is NOT SUFFICIENT

@bluvg

As I stated before, it is not sufficient to add a prompt for the UAC level settings dialog. This dialog is just one example of using "certified for auto-elevation" applications/dialogs to render the new UAC level useless (although it is an extreme example).

A malware could still turn off the firewall, make changes to system folders and mess around with other sensitive system settings at standard UAC level. An additional prompt for the UAC settings dialog just prevents the malware from turning off UAC completely (at least if malware cannot use the sending of keystrokes to change registry keys).

Thursday, February 05, 2009 6:21 PM by hux

# re: Update on UAC

Jon, the whole premise of a software is not malware if the user clicks "Allow" is bogus. Users do that all the time with hundreds of pop-ups and dialog boxes they are exposed to on a daily basis. Microsoft's attention should be to insure that malware cannot be installed or allowed to run on the system period - user allowed or otherwise. Microsoft has access to the same virus/spyware/malware definition databases as all the other anti-something vendors, so run a check to see if the software is listed before allowing anything to happen. If the user isn't online, quarantine the program until they go online to run the check, or cache the definitions on the system for it to refer to. Users are dumb, and security planning needs to be developed around that key fact.

Thursday, February 05, 2009 7:12 PM by LinuxGuyInRI

# re: Update on UAC

feedback today. I encourage everyone to read that. I am sure many people will be very happy!

As I described in my post, we will continue to listen to the feedback and improve our design of the UAC feature.

@Thack: Thank you very much for your post! I was hoping that I was going to be able to reach people who could understand our reasoning and then provide clear feedback in that context.

@mechBgon: Thank you for this feedback on better ways to measure malware infestation. It is very constructive. We only had defender in the sample study. We will be sure to use better sources for the beta study.

@artfudd: Please be fair. I am glad to share my point of view transparently and accept the full criticism from the community (some posts get more criticism than others :-)). I won't claim our data gathering is perfect, but it is valuable to understand what is really going on vs. what we think is going on in the real world. This does not diminish our desire to hear from and be responsive to our beta testers.

Some of the comments are attributing sentiments to me in the post that I did not intend. I sincerely apologize for any bugs in the post. I hope that taking the time to explain our thinking is not automatically assumed to be closed minded. I will work on my ability to put myself more in your shoes when I communicate in the future so that my communication is clearer. I remain sincere in my statement that we are listening carefully to the all of feedback and that we will use it to improve the UAC feature.

Thank you again for engaging with us and helping us make Windows 7 great!

Jon

Thursday, February 05, 2009 7:18 PM by jondevaan

# re: Update on UAC

Jon,

I have a simple question:

What is the security benefit of using the "Notify me only when programs ..." as opposed to "Never notify"?

Think about it:

Malicious or compromised programs can change the UAC setting or even worse [1], simply use a trusted Windows binary like rundll32 to run arbitrary code with full privileges without ever asking for elevation.

You say that "The most effective way to secure a system against malware is to run with standard user privileges." and I agree.

I'd argue that UAC *is* a security boundary, but only with "Always notify". Anything else and the prompts become completely optional for programs. Good programs will do it as a courtesy to the user, bad programs won't bother.

Here's a prediction: Sooner or later there are going to be 3rd-party programs that use the rundll-hack whenever they feel like they need administrative privileges. Makes programming much easier, without any pesky prompts for the user... and we're back to pre-WinXP-SP2 times.

[1] http://www.withinwindows.com/2009/02/04/windows-7-auto-elevation-mistake-lets-malware-elevate-freely-easily/

Thursday, February 05, 2009 8:19 PM by mx.2000

# re: Update on UAC

on two laptops and don't want to downgrade to XP for the warranty, and most of the time its OK, but some of the time it cant find some or even a lot of the hardware. so I follow the basic steps for finding before and after a restart LOL. I have looked deeply into the UAC in windows 7 and have some issues but nothing like being said from some people I love win7 it will smoke the OS Vista, in security and usability. all I can say to the ones responsible for this blog is get over it,yourself and grow up. This is not high school. I see nothing wrong with setting your own security for apps or installs, easily done with a few up grades to the windows system and cheap or even free and most of the public can find any of this info on THE WEB. Windows needed a foothold and have my hand as one. I feel it necessary to help out my big brother when I can and they have me and my business with the software's they offer. all anyone needs to know they screwed up with VISTA and they know it get off the back of a friend in software. they are and always will be the OS leader in the world.

Thursday, February 05, 2009 9:35 PM by rcpoll@msn.com

# re: Update on UAC

Jon,

Perhaps you need a different perspective on this UAC situation. Bryant of AeroXP, a Windows Enthusiast Community of which I am proud to be a member of, has written a great article. I will provide the link for you.

http://www.aeroxp.org/2009/02/the-real-issue-with-win7-uac/

This really explains why an easy disabling of the UAC can be so problematic.

As Bryant said, it could be common downloadables that are hijacked to compromise the UAC. The recent incidents with pirated software that hid trojans in Mac software should be the first reason for change. Pirated iWork and Photoshop CS4 with trojans, could easily be a podcast or some other legit program. That is why the UAC has to be much stronger. VB is taught my old high school. With practice and internet resources, some high school kid and a genius intelligence could compromise the UAC. That is why I'm glad you guys are taking a second look at this.

The simple answer is this. UAC to most folks represents a level of security in Windows 7 and Vista. To dismiss that is leading many people into a false sense of security. As for me, I do not. That is why I have anti-virus, a router with encryption and a firewall, a program to cleanup both Registry and programs, and I check Windows Updates on a DAILY basis. I check software updates on a WEEKLY basis. I have a routine that I have developed since my first copy of Windows XP. This routine has helped me avoid Blaster, Sasser, Conflicker, and many of the worms out there.

Most folks don't do that. They browse and click on things with ignorance. Windows 7 has to consider the uneducated user who just clicks and doesn't think. It has to provide a greater defense, balanced with not annoying the piss out of an average user. Its something that both OS-X and Linux has mastered.

However, I have to agree with LinuxGuyInRI. Using a combination of white lists and black lists of programs, known viruses, known virus techniques, and other patterns of malware, Windows 7 can have a much stronger defense. Windows 7 needs to neutralize these black listed ones before they find a place on the Hard Drive. Thats just common sense in my opinion.

I really do appreciate your hard work Jon. If I had the expertise, I'd be working for you guys. I'd love to be in the thick of creation of a new OS. I don't envy the tough choices you guys are having to make. However, as you can see by the interest, people want Microsoft and Windows to be a huge success.

Thank you, God bless, and Good luck. Also, big thanks to Steven Sinofsky for the blog.

Thursday, February 05, 2009 9:40 PM by hitman721

# re: Update on UAC

I
S
U

NO OTHER CHANGES TO W7 UAC ARE NEEDED! I can't believe that MS doesn't get this...boggles my mind.

If MS leaves W7 the way it is, UAC is completely worthless and should be removed from the OS.

Thursday, February 05, 2009 10:07 PM by yngdiego

# re: Update on UAC

So the only problems seem to be that the default setting of "Notify me only..."

1) allows UAC level to be changed by a non-elevated malicious program

2) is easily exploited to elevate malicious programs

It's alright to trust your research that this is the best balance, but we users are just asking Microsoft to FIX this setting.

Friday, February 06, 2009 4:57 AM by teoh.hanhui

Anonymous comments are disabled