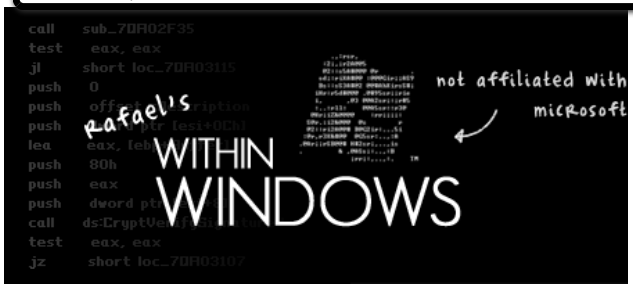

UAC, UAC, go away, come again some other day

committed to database on June 10, 2009 at 6:46 pm Eastern Standard Time digg this 37 comments

I was reading Mark Russinovich's latest UAC article and Long Zheng's latest scribblings and... developed quite the headache. Honestly, I'm tired of trying to sort out what UAC really is and don't care anymore. UAC has become this gigantic undocumented blob of an idea that is explained (differently) on-demand every single time, to fit some marketing agenda du jour, and I'm sick of it. Mark jumps up and down about how UAC isn't a security boundary and how we're stupid for thinking such, yet Microsoft's own sites pitch otherwise. Whatever, guys.

Here's my million dollar question: If UAC wasn't designed to ultimately protect us from anything, **why does its icon resemble a damn shield?**

Tim Foote
June 10, 2009 at 7:10 pm

I would just like to say that UAC is a pain in my ass and it's the first thing I disable when installing Vista or 7.

I think they should change the shield icon to a demonic troll or something of the sort as that's the way it behaves on a good day!

Dan
June 10, 2009 at 7:17 pm

Maybe they're trying to protect the system from the user. :)

Brad
June 10, 2009 at 7:32 pm

So should we just not use UAC then?

Leo Davidson
June 10, 2009 at 8:18 pm

http://blogs.msdn.com/uac/

"User Account Control (UAC) is a core security feature in the next release of Windows Vista and Windows Server code name Longhorn."

https://blogs.technet.com/jesper_johansson/archive/2006/06/22/438316.aspx

"Once the OS is released, if you absolutely can't stand a security feature that is designed to protect you, by all means, turn it off"

etc.

Mark Russinovich has been more consistent, I think, but I used to get the impression he was saying that UAC was a security feature that wasn't as good as an actual security boundary but was better than nothing and tried its best. Now it seems we're (sometimes) told it isn't even a security feature. UAC is for convenience and annoyance, or something. The convenience of being annoyed for no reason.

Recent Posts

Tweak your Windows 7 Logon UI "button set"

UAC, UAC, go away, come again some other day

Inside the Touch Pack for Windows 7: Blackboard

Inside the Touch Pack for Windows 7: Rebound

more annoying than admin accounts in Vista, which MS know were too annoying for too many people to use. If MS are serious about standard user accounts being the goal then they have a lot of work to do, particularly in making Explorer and the Control Panels show fewer prompts. Instead MS have made admin accounts more tempting with Win7, not less. Fail.

http://www.techsphere.org/wordpress/2007/05/08/microsoft-withdraws-vista-security-claims/

"Russinovich's talk was supposed to give professionals an idea of how to work with UAC in order to avoid excessive pop-up warnings and avoiding breaking the UAC model."

^^^ I think Mark should've given that talk internally! Clearly the Explorer/shell team missed the memo as their code produces excessive pop-ups and required Microsoft to break the UAC model in Windows 7 as a workaround which nobody else is allowed to use. Utter fail.

Dominik
June 10, 2009 at 8:33 pm

"...why does its icon resemble a damn shield?"

lol

Mopeto
June 10, 2009 at 11:29 pm

I lol at people who, argue "That thing is fucking anoying, is horrible, etc etc" but then they got fucking malware, virus, etc and blame microsoft on poor security, damn.
I only use Common Sense 95 and even not antivirus and I don´t get fucking plague.

Mattisdada
June 11, 2009 at 12:02 am

I agree with what Mopeto is saying, although fairly badly said.

As long as you use some good old fashion sense, you will be RELATIVELY safe. If you only download from trusted sources, have a firewall of some sort (hardware, or software). You will be pretty safe.

If you say, go to lots of warez pr0zn sites and the such. You will easily get allot of malware on your computer.

The problem is allot of, novice, users do stupid things. Windows needs to be more idiot proof.

For example, 99% of novices, NEVER read what a popup is, they just press a button (a random button). And i do believe that UAC makes this worse. The biggest threat is the dumb user, not outside entities generally. And the dumb user will let IN the outside entities.

I do believe Microsoft needs to keep this in mind. "Power" users are generally fine. If we DID get malware, it does less damage, and we can quickly neutralize it to some extent without an AV even.

Resle
June 11, 2009 at 12:39 am

> If UAC wasn't designed to ultimately protect us from anything, why does its icon resemble a damn shield?

It's not a shield: http://image55.webshots.com/55/4/80/17/545248017SNMPdt_ph.jpg

Jody
June 11, 2009 at 12:45 am

As they say in other places this auto-elevation (and code injection) is only a problem if you are running in an Administrator account. Run as a standard user and none of this is a problem, you will always be prompted for elevation.

pin
June 11, 2009 at 1:32 am

in fact in Win7 they changed the colour like to say now it protects less than Vista.

concept, white paper made available

Short: Windows 7 Release Candidate now available to all

Short: Windows 7 Release Candidate auto-elevate white list

Short: vLite screws up Windows Vista SP1 upgrade path

Windows XP Mode Internals – Part 2 (Application Publishing Magic)

Windows XP Mode Internals – Part 1 (Overview)

Secret No More: Revealing Windows XP Mode for Windows 7

Wish Long Zheng a Happy Birthday

Rumor smash: Windows 7 will keep 6.1 versioning

Photo Sharing feature in Live Messenger: Kill it dead

Less obscure Microsoft Office 14 64-bit evidence

Offbeat: Buy.com and Nokia hate the environment, apparently

Windows 7 to support third-party codecs... like all other Windows versions

Correction: Starter wallpaper more secure than I thought

IE 8 slow? This tweak won't help.

Badges

@Jody:

a) Running as standard user brings pretty much all the UAC prompts that were in Vista back.

b) On top of that, you have to type a password rather than click a button.

Microsoft clearly realise that even the button-click prompts were too annoying for many users as that's why they removed them for admin users (for their badly-written software which prompts too much only).

You cannot honestly thing that standard user accounts, as they stand today, are a solution that people will actually use after the reaction to Vista's UAC.

Additionally, standard user accounts are not the default. You have to go out of your way to use them. Almost nobody will, except in businesses where they were already running locked-down accounts since the days of NT4 and where UAC elevation will barely be used at all.

Standard user accounts are a distraction and an excuse as far as Windows 7 goes. You might as well say "People should use Linux to be more secure" as it's about as relevant and likely to happen. If Windows 8 (or whatever) actually makes standard user the default, and makes improves the user experience to one that people might actually put up with, then the argument will hold water.

The thing is, we're only arguing about the stupidity (and unfairness on 3rd party developers) of Windows 7's UAC because of the default settings. People can change to Always Prompt and make it like Vista… Unless we explain why Windows 7's defaults are the worst of both worlds — annoying prompts for some applications combined with almost zero difficulty in bypassing the prompts for anything that really wants to — and inform people that they can either set UAC to always prompt or to silently elevate (for all apps), people are just going to use the defaults.

The one thing most people are not going to use in Windows 7 is standard user accounts. It's more painful than what everyone complained about on Vista, not less.

John Sedlak
June 11, 2009 at 3:35 am

What are you guys doing that requires elevation so much? I always held onto the idea that UAC was there to be a checkpoint whenever software wanted to change the system in some way. Unless I am installing something or moving files into the system directories, I very rarely run into the prompts.

If anything, I think UAC should get tougher on software. Each process should be run in isolation from everything and when another process wants to come into that space or that process wants to move out, show a prompt with the two processes causing the problem.

Leo Davidson
June 11, 2009 at 5:54 am

I don't think it's supposed to resemble a shield (or the firewall icon etc.)…

The new Windows 7 UAC logo has just been unveiled:

http://www.pretentiousname.com/misc/uac_comedy_tragedy_security_theatre.png

:-D

MagicAndre1981
June 11, 2009 at 6:25 am

Hi Leo, what about releasing a demo app? This will impose pressure upon MS to fix it

Leo Davidson
June 11, 2009 at 7:05 am

I've decided not to release the demo app for now (except for a handful of people to verify) because I think it's more likely MS would just break that particular demo app (which they could do quite easily, e.g. block the exe via Windows Defender) rather than address the underlying issue.

That'd mean I'd have to waste time making another demo app which proved the hole still existed. I'd rather spend my time on something more constructive (or editing my monstrosity of a webpage :)).

hasn't been talked about in public yet and makes it easier to turn the main "copy a file" thing into "run anything elevated").

anonymous
June 11, 2009 at 7:25 am

I'm now convinced that the Explorer team is the worst amongst the various Windows teams.

Horseradish
June 11, 2009 at 8:17 am

I'm with Brad. I disable UAC in group policy and use "safe surfing" and other best practices to keep my system secure. UAC has a false security, and I'm more vigilant and respective of security when I don't rely on anything else to keep me safe.

Marty
June 11, 2009 at 9:19 am

UAC is a security FEATURE, not a security BOUNDARY. That's a technical term that is more than just semantics.

Personally I don't see what the big deal is. What are you doing that requires so much elevation? I can understand disabling UAC while building a system, but after that turn it back on. If you have apps that you always run elevated, setup a scheduled task and run them at startup, or on demand with a shortcut. This has been documented since Vista was in beta. If you do a lot of file system work, create a scheduled task for cmd.exe or powershell.exe to run elevated at startup, and use that for copying/moving/deleting.

I've been using the same desktop system since Vista was in beta, and I don't even have anti-virus installed. I leave UAC enabled and rarely see a prompt. This system has never had a virus infection, runs fast, no crashes, and only gets rebooted once a month when patches require it. And I've never rebuilt it, it was only rebuilt for the final RTM code, rather than upgrading over several beta upgrades.

Sameera
June 11, 2009 at 9:30 am

"why does its icon resemble a damn shield?"

You know, if you squint a bit and concentrate really hard, you can make out what that symbol really is…

It's Steve Ballmer's right hand giving you the finger…
:D

Stephen
June 11, 2009 at 10:17 am

That icon isn't there to represent what UAC is or what it does for the user. It's there to be found by Link for use against Ganon, protecting the princess and the Iraq and U.S. Americans and everywhere like, such as. DUH, RAFAEL! GET IT RIGHT! UAC FOREVAR! lol.

-Stephen

Leo Davidson
June 11, 2009 at 10:20 am

@Marty:

"UAC is a security FEATURE, not a security BOUNDARY. That's a technical term that is more than just semantics."

Microsoft seem to be claiming it isn't even a security FEATURE anymore. That's their excuse for creating bigger holes in it instead of closing off the existing holes (which are also used as an excuse: "The old system wasn't perfect so new flaws don't matter!").

"Personally I don't see what the big deal is. What are you doing that requires so much elevation?"

The big deal is that the default Win 7 settings are the stupid combination of prompts for 3rd party software and next to no enforcement of those prompts. The only time you'll see a prompt is if the app didn't want to hide one from you, essentially.

On the other hand, people who do get annoyed by all the prompts will still be annoyed by the ones for third party programs (as well as stuff like the Sysinternals tools).

People who run standard user accounts but are still the computer's administrator will continue to be annoyed by lots of UAC prompts where they have to type the password each time, sometimes several times while dealing with the same folder or whatever (unless they use a 3rd party file manager which handles UAC in a nicer way).

The point isn't that you can configure things to be as secure as they were; it's that the new default configuration is completely stupid to anyone who stops and thinks about it. And Microsoft keep moving the goalposts to suit their argument. (e.g. They don't care that this hole to bypass the prompts exists, yet they refuse to allow a proper system to whitelist third-party code because allowing third-party code to bypass the prompts* would be bad. What the hell kind of logic is that?)

(*I'm talking about the prompts, not the entire UAC API. Making apps use the API to gain elevation is a good idea. Hassling the user with a prompt which is easy to bypass is a stupid idea.)

richard
June 11, 2009 at 2:00 pm

Leo Davidson, you should post to channel9. There is a thread about this going on, with some MS developers to boot:
http://channel9.msdn.com/forums/Coffeehouse/473037-UAC-controversy-the-last-episode/

Eldarien
June 11, 2009 at 3:32 pm

"The one thing most people are not going to use in Windows 7 is standard user accounts. It's more painful than what everyone complained about on Vista, not less."

This is absolutly not true in a "more painful" part. I am using limited accounds in XP for a long time (and now in 7), and if in XP you have to run setup.exe as admin manually, 7 will ask you to run as admin — that's the one and only "painful" part. There are nothing painful in everyday work after all software installed and configured. Also, this is much more secure and I think is the only right way. It just needs a little more work for better user friendlyness.

xaml
June 11, 2009 at 7:23 pm

lol

Leo Davidson
June 11, 2009 at 8:53 pm

@Eldarien: If you were willing to put up with standard user on XP then good for you. Please realise, though, that if everyone else was like you then Microsoft would not have had to change UAC in Windows 7 at all because UAC in Vista would've been perceived as absolutely wonderful by everyone.

It wasn't.

Leo Davidson
June 11, 2009 at 8:57 pm

...besides which I was comparing Vista/Win7 standard user prompts to Vista admin prompts. They are more painful; how can you deny that? You have to type a password instead of click a button.

Sure, they are less painful than switching users on XP was, but that's besides the point. I'm not arguing for UAC to be ditched entirely.

Leo Davidson
June 12, 2009 at 9:27 am

@Myself: "I've decided not to release the demo app for now"

I had a change of heart, after recent discussions with people on all sides of the issue. Source and exes are on my website now. Long has also put up a new article with a video demonstrating it running on the RC build.

June 12, 2009 at 12:50 pm

I saw Long's video: Very well done to explain the overall idea.

I read Leo's source-code comments. Helpful, but, Leo, where's your video to go with it?

I'm a programmer (VB, etc.), but I have never used C++, as it gives me a headache. Still, I wouldn't mind a guided video walkthrough of Leo's code by the master himself.

GOOD JOB, GUYS!

Leo Davidson
June 12, 2009 at 3:25 pm

"Helpful, but, Leo, where's your video to go with it?"

My videos are here: http://www.pretentiousname.com/misc/win7_uac_whitelist2.html#videos

"Still, I wouldn't mind a guided video walkthrough of Leo's code by the master himself."

Ah, if you want a video going over the code then there isn't one, but check out the readme file that comes with the code for a point-by-point description of what it does.

Everything that the code does uses standard techniques which are well-documented on the web. (e.g. Look up articles in MSDN, CodeProject, etc. on "code injection".) So there's nothing really novel going on, except what's described in the readme.

If you look at the source code, the interesting stuff is in the *_Inject.cpp file, and a little in the Utils file. Most of the other code is boring GUI stuff that will only bog you down.

el_bot
June 12, 2009 at 6:03 pm

Don't forget that malwares isn't the only threat. There are shell codes, remote exploits, etc (take a trip by milw0rm if you disagree). Open a document PDF with a shellcode embedded under XP and you will notice the difference…
Anyway, in the world Windows, the main threat is the user: every thing that try educates it ,a priori, is fine.

KsbjA
June 13, 2009 at 4:16 am

The right question is not, whether UAC was designed to protect something. It was, undoubtedly. The only question is, if it actually does that.

Leo Davidson
June 13, 2009 at 6:39 am

The source code is now online in HTML format as well. Start here:

http://www.pretentiousname.com/misc/W7E_Source/Win7Elevate_Inject.cpp. html

I also converted the step-by-step guide in the readme into HTML:

http://www.pretentiousname.com/misc/W7E_Source/win7_uac_poc_details.ht ml

Now you don't have to download the source zip or have Visual Studio to see how simple it all is.

Leo Davidson
June 13, 2009 at 6:40 am

(Oops, URLs got mangled in my clipboard. Correct ones here.)

The source code is now online in HTML format as well. Start here:

http://www.pretentiousname.com/misc/W7E_Source/Win7Elevate_Inject.cpp.html

I also converted the step-by-step guide in the readme into HTML:

CDan
June 13, 2009 at 6:08 pm

Actually I like UAC... gives me a feeling of 'nuthnz happenin behind my back..(that I don't wan to happen) '

Name (required)

Mail (will not be published) (required)

Website

Submit Comment