

# Re: Security and the User experience

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-08/msg00235.html>

---

- *From:* "Rob R. Ainscough" <[robains@xxxxxxxxxxx](mailto:robains@xxxxxxxxxxx)>
  - *Date:* Wed, 26 Jul 2006 08:00:57 -0700
- 

MSN doesn't seem to have a problem with this? I don't think capacity will be an issue and don't forget your not looking at massive amounts of data — just one secure token.

Microsoft, Apple, \*nix can say all they like, but the consumer will simply say NO it isn't our responsibility and just NOT consume. Until these companies assume the responsibility (at least from a logical/software perspective) they will NEVER go beyond the current market share. A good case in study will be seeing how XBOX360 works with "users" since these users tend to be the people that avoid the hassle of playing games on a PC. However, on the business side, we have a huge client base of users that don't know how to secure, nor way they should secure, nor how to deal with security messages that are tossed at them either by Windows firewall or some other third party anti-virus software. Many of the drone hacked PCs out there doing the bidding of hackers are exactly from users that don't implement any security and/or just have no clue about security on their PC.

There needs to be a solution because you can't force a consumer to do anything. Continuing the ignorance really has limited the market appeal of PCs. The time and resources needed to implement this concept will be high, but the long term will be so much better for ALL involved. Hell, even charge the companies producing the applications (i.e. my company) for the authentication token (just how Network solutions charges for a DNS lookup or Verisign charge for SSL certificates).

The solution exist, but if we don't come up with some other than "it's the user's responsibility" then 1 in 5 people will be our fate, it'll never grow. Besides what is Bill Gate's net worth these days 40 billion, 60 billion, 90 billion — the money is there to make it happen.

"Patrick Dickey" <[pd1ckey43@xxxxxxxxxxxxxxxxxxxxxx](mailto:pd1ckey43@xxxxxxxxxxxxxxxxxxxxxx)> wrote in message <news:OZptghFsGHA.1976@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

"Rob R. Ainscough" <[robains@xxxxxxxxxxx](mailto:robains@xxxxxxxxxxx)> wrote in message <news:OV2maQAsGHA.4004@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
My answers are inline with yours...

## Re: Security and the User experience

The problem:

User installs an application that needs to communicate to SQL servers and/or FTP servers and/or web services. Being a good user they have some type of firewall and anti-virus software (most of the time it is preconfigured so the user doesn't even know what they have). The problem, whenever the user installs any applications (or even games) they are either presented with a message saying "block/unblock" message and sometimes even messages suggesting the application could be a virus. So the user doesn't really understand this message at all and could pick either option or just ignore the message entirely (and in many cases with games, the message is hidden behind the full screen DX9 game so the user is completely unaware until after then exit the game wondering why it doesn't work. In some cases the firewall/anti-virus software will not even provide a prompt and just block the application 24/7. As a result the application may not work and/or the user can't play online and you get one very frustrated user (either in a work environment or a home environment). In fact, users get so frustrated that they stop using their PC and move on to other things in life.

Microsoft do seem to be aware of this user experience problem after my initial look at Beta 2 of Vista and how it grays out everything except the program needing communication. Unfortunately, this is still "in the way" for your average user and I don't believe this will help increase the PC base of users. We've been hovering at 1 in 5 people having computers for a long time now so there is obviously a large "market share" to tap into.

I have a possible solution:

Any application that will be released on a public level should register itself with an authority. The OS will then query the authority whenever any application is installed, if the application has been validated by the authority installation, then communications will be permitted for that application. This process could become automated (similar to how SSL certifications are acquired) at trusted companies/sites. What this does is provide user confidence and at the same time insulates them from having to deal with security.

While this is a good idea in theory, the resources that it would require are too great. If 1 in 5 people are using a computer, and they all try the same (or different, for that matter) application at the same time, it would crash the 'authority'. The authority that would hold this information would have to have a backbone to the Internet, and would have to have a lot of servers to handle the load. Before anyone says that Microsoft has that capability, they don't. It would be a little more in-depth than just going to hotmail and getting your e-mail. They would have to set up servers all over the world, and have them all replicate the information at the same time.

## Re: Security and the User experience

I think Microsoft really need to smell the coffee here, because their path of "that's just the way it is" does nothing for anyone involved in the business of PC's and software development. What I'm seeing in Vista is better, but doesn't go far enough to insulate the user from security. In fact, in Microsoft's own book(s) on security, they clearly identify that security should NOT be in the way. I for one would like to see even a modest increase in market share from 1 in 5 people to 2 in 5 people (that's effectively doubling market share) -- this is good for everyone. What Microsoft are failing to do is accept the reality of their situation (you can't tell the user it's their job to ensure their secure, they will just simply say no it isn't and stop using the PC -- not up for debate period), sure it will require more work, more money, and new "entities" to manage my proposed solution but the long term benefits will easily pay off and since we already have entities that do very similar functionality (Verisign, Networksolutions, etc. etc.).

What do you think?

Rob.

I would tend to agree with you about Microsoft needing to smell the coffee. And to an extent, they are. However, the \*nix OS's have basically the same feature (albeit not as intrusive as UAC) called "superuser". Microsoft is just trying to make a variation of that, but it's still too intrusive. I would venture to say though that even the \*nix OS' distributors and probably even Apple will still say that it's the users job to make sure their computer is secure.

Before I get flamed for the last sentence, let me clarify it a little. Yes it's the responsibility of Microsoft, the \*nix distributors and coders, and Apple to provide us with secure code. But, it's up to the end-user to make sure they get the updates that will make the code (and their computers) secure. It's also up to the end-user to do whatever is necessary to make sure their computer is secure (meaning antivirus, firewall, and antispysware).

You are right though that something has to be done. If it wouldn't be too unmanagable, and if there was a foolproof way to ensure that the system wouldn't be violated, I would completely agree with your concept.

--

Patrick Dickey.

smile... someone out there cares deeply for you.  
<http://www.microsoft.com/protect>

Re: Security and the User experience

<http://update.microsoft.com>

<http://www.pats-computer-solutions.com>