

Re: Security and the User experience

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-08/msg00006.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Tue, 25 Jul 2006 19:46:23 -0700
-

Thoughtful analysis and interesting proposal, but I doubt it would fly.

I watched as MS at the end of the beta for XP trimmed down the firewall capability so that it allowed any outbound traffic. They received much harsh feedback for this, but basically said, amongst other things, that the user experience with other firewalls from "popup notices" etc. was not at all good, etc. and that they were avoiding that. A little time passed and we are now back over on the other side.

If there were a central authority such as you suggest, then who funds it, how do I know that I should actually trust it, how much does it cost me to verify to it that what I want registered should be registered, etc..??

Roger

"Rob R. Ainscough" <robains@xxxxxxxxxxxx> wrote in message news:OV2maQAsGHA.4004@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

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.

Re: Security and the User experience

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.

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.