

Re: Registry questions....

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-10/12044.html>

From: Jim Hubbard (*reply_at_groups.please*)

Date: 10/11/04

Date: Sun, 10 Oct 2004 21:21:18 -0400

Thanks to Will, Michael and HillBillyBuddhist for their pointers.

The solution I had was a \$60 PCI card that locks down the C: partition. And, it REALLY locks it down.

For example....if you change the default fonts of an application, or you change the return email address in Outlook, all works fine until you reboot. Upon rebooting, all of your changes are gone.

While this makes for a very stable (i.e. Virus-Proof) system, it does not make for a user friendly system. You have to allow the users to control the allowed applications while not allowing unapproved applications (i.e. viruses and such).

XP has the security built-in to do this, but there is no user-friendly ("dumbed-down") interface for this. Also, it requires that a user NOT run his/her PC using the Administrator account. Doing so poses security threats that you can avoid if you only use the Administrator account to install applications and tweak your security settings and use a Power User or User account for running your applications.

This works well in a business environment - where the Administrator is usually an IT person and the users don't have access to the Administrator account. But, home users like to install and uninstall applications frequently (at least I know I do) so it may not be so user friendly for the way they like to operate their home systems.

I'm documenting how to lock things down using the built-in XP tools, and I may try my hand at making a simple user-interface for it later....after I work out exactly how it works.

BTW, I work with users at 9 different small businesses (will be 10 starting this week) as their System Administrator (or "computer guy"), and they tell me that applications (like Tea Timer, RegProt and even McAfee's Firewall) that pop-up warnings mostly cause more confusion because they don't know whether they should allow an application to continue or not. Most of the confusion comes from the cryptic names given to the executables that are

shown to the users.

These are USERS. They don't know that MS has services that need access to the network through MacAfee's firewall. "And what the hell is a service anyway," one of them asked me the other day. Sometimes I don't even recognize the app that is asking for access to whatever.

What we need is simplification. We need to dumb that crap down so that I can still do it right with a head-cold and 2 shots of Nyquil in me.

Why don't all major code publishers use certificates to identify themselves give a title/description of their app that any user can understand? The simple fact is that most people don't give a rat's ass about learning how the computer and security work. They just want to play a game, or build a house, or balance their checkbook. So how could we make this easier for them? I have an idea.....but it needs some more fleshing out first.

Thanks for your help!

Jim Hubbard

"HillBillyBuddhist" <hillbillybuddhist@shoescolumbus.rr.com> wrote in message news:OSTjl4xrEHA.1204@TK2MSFTNGP12.phx.gbl...
> "Jim Hubbard" <reply@groups.please> wrote in message
> news:5jhad.208875\$Np2.166691@bignews4.bellsouth.net...
> |I am asking because I want to lock down my PC to prevent viruses and
> such,
> | but some registry entries need to be left open for program use.
> |
> | I can lock the whole PC down just fine, but there goes any customization
> of
> | applications while it is locked down.
> |
> |
> |
> You might consider Regprot.
> |
> "RegistryProt is a 100% free, standalone, compact, low-level realtime
> registry monitor and protector, that adds another dimension to Windows
> security and intrusion detection. By monitoring important locations and
> keys
> in the Windows system registry, RegistryProt will alert whenever a key is
> added or changed, and then give the option of accepting the key change,
> reverting back to the original key setting, or deleting the key."
> |
> It doesn't "lock down" the registry per se but it does give you a better
> handle on what gets added.
> |
> |
> | <http://www.diamondcs.com.au/index.php?page=regprot>
> |
> |

> --

> *D*

>

> *I'm not an MVP a VIP nor do I have ESP.*

> *I was just trying to help.*

> *Please use your own best judgment before implementing any suggestions or
> advice herein.*

> *No warranty is expressed or implied.*

> *Your mileage may vary.*

> *See store for details. :)*

>

> *Remove shoes to E-mail.*

>

>