

Re: How can I identify a system uniquely using MFC code

## Re: How can I identify a system uniquely using MFC code

---

*Source:* <http://www.tech-archive.net/Archive/VC/microsoft.public.vc.mfc/2006-06/msg01198.html>

---

- *From:* Joseph M. Newcomer <[newcomer@xxxxxxxxxxxxx](mailto:newcomer@xxxxxxxxxxxxx)>
  - *Date:* Wed, 14 Jun 2006 23:53:06 -0400
- 

If my laptop is stolen, there is no security issue, because I make it a point to never keep proprietary data on my laptop. I carry a little external hard drive, which I keep in my pocket, and that's where I keep proprietary information; it is only plugged into the laptop if I'm using the laptop. Otherwise, the two are kept separate.

The Internet solution doesn't help if you're trying to use a product at 35,000 feet over Nebraska. At least not until airlines start supporting reasonably-priced broadband (and I hope they don't because of VoIP).

The official definition of "Copy Protection" is "A class of methods for preventing incompetent pirates from stealing software and legitimate customers from using it. Considered silly."

Don't worry—NGSCB will save us all!

(and if you believe that the Next Generation Secure Computing Base will actually make systems more secure, you are almost certainly interested in my wonderful beachfront property in New Orleans. Well, it isn't beachfront YET, but it will be after the next hurricane. Buy now!)

The TCB (Trusted Computing Base) does solve some important problems in computer security, but it will NOT make our computers safer, or prevent viruses, or any number of other myths I've heard people claim will be true (alas, some of them even work for companies involved in trusted computing projects...and I can't say too much about one of them because I just invested two years in a project I can't talk about yet)

joe

On Wed, 14 Jun 2006 16:12:39 -0700, "Ed Weir \((ComCast\))" <[Anon@xxxxxxxxx](mailto:Anon@xxxxxxxxx)> wrote:

"Joseph M. Newcomer" <[newcomer@xxxxxxxxxxxxx](mailto:newcomer@xxxxxxxxxxxxx)> wrote in message [news:r0ft82drh8qds83lii8ltdke71nc42bpd@xxxxxxxxxxxx](mailto:news:r0ft82drh8qds83lii8ltdke71nc42bpd@xxxxxxxxxxxx)  
| You point out the absurdity of most hand-rolled "copy protection" schemes.  
| Look how much  
| more complex your solution is, and I suspect it is just a beginning, based  
| on some of the  
| consulting I've done. The actual copy protection means in most  
| proprietary products is

Re: How can I identify a system uniquely using MFC code

Re: How can I identify a system uniquely using MFC code

| considered secret for obvious reasons, but I've worked with several clients who thought  
| they'd "solved" the problem on their own ("we don't need to spend money on some commercial  
| product!"), and I was able to demonstrate ways of cracking their schemes within a day (I  
| used to have an anonymous account that I used to lurk on cracker newsgroups. Anyone who  
| thinks they can roll their own copy protection scheme should do this first. Discover how  
| trivial it is to crack ANY software-only scheme. Realize that even the best commercial  
| software-only products, written by experts in these areas, are highly vulnerable. Then  
| give up and get a hardware-related product with a dynamic challenge-response mechanism and  
| high-level encryption, and you MIGHT have a chance of keeping your software secure...)  
| joe  
|  
| On Mon, 12 Jun 2006 20:06:05 -0700, "Ed Weir \((ComCast\)" <Anon@xxxxxxxx>  
wrote:  
|  
| >"Bruno van Dooren" <bruno\_nos\_pam\_van\_dooren@xxxxxxxxxxxx> wrote in message  
| >[news:ug75QYgiGHA.3440@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:ug75QYgiGHA.3440@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)  
| >> I am working on a MFC application. I need to identify every  
| > > system which uses this application. How can I do this using MFC? Is  
| >there  
| > > any unique identifier for a PC which can be retrieved using MFC?  
| >|  
| >| You can find the computer SID in the registry.  
| >| More details over here:  
| >| <http://www.sysinternals.com/Utilities/NewSid.html>  
| >|  
| >| —  
| >|  
| >| Kind regards,  
| >| Bruno van Dooren  
| >| bruno\_nos\_pam\_van\_dooren@xxxxxxxxxxxx  
| >| Remove only "\_nos\_pam"  
| >|  
| >| >This use of an SID is woefully inadequate for security, as the site you  
have  
| >referenced illustrates so well; anyone can change the SID of a computer,  
so  
| >how can we expect the data on our hard disk to be secure? This is just  
one  
| >more example of dangerous security assumptions and coding done by the  
| >'experts' at MSFT.  
| >

Re: How can I identify a system uniquely using MFC code

|>A more secure method would be to create a one-way sha-256 or AES-256 hash  
|>of:  
|>1.) volume ID + SN  
|>2.) User ID  
|>3.) User domain  
|>4.) Machine name  
|>5.) OSINFO  
|>6.) User PIN or passphrase  
|>  
|>to lock the user to the hardware in use. In the event of a hardware  
failure  
|>the last element can be used to recover the ID if necessary. There is of  
|>course more to it than this, certain code which needs to be written to  
|>implement the hash and to later validate it as well as to recover the ID  
|>after hardware failure or machine migration.  
|>  
|>Point is, the SID is anything BUT secure...  
|>  
|>-- Ed.  
|>  
|>-----  
|>hex->bin->b64  
|>F9E7707A2AF502D0A899C6ACB43A2D35EB7E  
| Joseph M. Newcomer [MVP]  
| email: newcomer@xxxxxxxxxxxxx  
| Web: <http://www.flounder.com>  
| MVP Tips: [http://www.flounder.com/mvp\\_tips.htm](http://www.flounder.com/mvp_tips.htm)

You nailed it. Only use the internet connection as your 'hardware', and a server you control as your 'dongle'. Since most applications are internet related, this will solve the problem for a good percentage of applications needing protection against piracy.

Secret methods are kept secret in complete ignorance of the principles of Applied Cryptography; you must always assume that an attacker has full knowledge of how your scheme works, and will (quickly) devise an attack if the target is worth the effort. You are only as secure as the cost of the attack exceeds the worth of the prize. You have succeeded in attacking your targets because of the relative ignorance of the victims. Unfortunately (for all of us), not a great feat.

The more complete solution would be to:

- 1) Educate every user in secure usage and practices
- or
- 2) Design systems that are intrinsically secure\* without having to depend on user competence in security

E.G.; What if your laptop gets stolen – is your data on it secure from attack?

I just got a letter from the Gov't that my service information has been

Re: How can I identify a system uniquely using MFC code  
compromised. How did this happen?

-- Ed.

---

hex->bin->b64  
F9E7707A2AF502D0A899C6ACB43A2D35EB7E

\* The cost of attack exceeding the value of the prize

Joseph M. Newcomer [MVP]  
email: newcomer@xxxxxxxxxxxxx  
Web: <http://www.flounder.com>  
MVP Tips: [http://www.flounder.com/mvp\\_tips.htm](http://www.flounder.com/mvp_tips.htm)