

Customizable security in NTFS? Needs to be extensible & dynamic

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2007-07/msg00351.html>

- *From:* Chuck Chopp <ChuckChopp@xxxxxxxxxxxx>
 - *Date:* Tue, 17 Jul 2007 10:41:46 -0400
-

I'm very familiar with the Win32 Security API functions for managing NTFS permissions. However, I've come up with a need to have a more dynamic way of updating the effective access rights to a folder or file on-the-fly. Since a user's access-token is generated at logon time, adding the user to new security groups doesn't alter the effective security until the logout and logon again. I also don't want to alter the existing DACL because there may already be other ACEs with the user's SID in them that provide some level of access, but the set of rules to be applied for determining allowed & denied access levels may change frequently and modifying ACEs that may be inheritable could impose an overhead on the system that's not acceptable in terms of resources spent propagating inheritable ACEs.

I'm looking into file system filter drivers in an attempt to determine if there's a way that a filter driver layered on top of NTFS would allow me to implement this more sophisticated type of security. It would appear that in Win2K3 R2, the file filtering and directory quota features are implemented as filter drivers rather than being integrated directly into NTFS itself, so I'm thinking that I'm on the right track here. However, it wouldn't hurt to get some confirmation from somebody with experience at writing or supporting the development of file system filter drivers.

Am I heading in the right direction? Or, do I need to look at "hooking" the API functions that determine effective rights?

TIA,

Chuck

--

Chuck Chopp

ChuckChopp (at) rtfmcsi (dot) com <http://www.rtfmcsi.com>

RTFM Consulting Services Inc. 864 801 2795 voice & voicemail
103 Autumn Hill Road 864 801 2774 fax
Greer, SC 29651

Do not send me unsolicited commercial email.

.