

## Re: [Updates] Re: More Before–The–Fact–Isms II

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-01/0940.html>

---

**From:** Karl Levinson [x y] mvp ([levinson\\_k\\_at\\_despammed.com](mailto:levinson_k_at_despammed.com))

**Date:** 01/22/05

Date: Fri, 21 Jan 2005 22:30:21 -0500

"Gordon Fecyk" <[gordonf@pan-am.ca](mailto:gordonf@pan-am.ca)> wrote in message  
news:eMiemeBAFHA.3120@TK2MSFTNGP12.phx.gbl...  
> *I've run into a problem and a solution with locking down the Execute  
> permissions in %userprofile%. If the %userprofile% ACL is not the default  
> (with the current user having full control over everything), Win2K can't  
> save the user's profile when the user logs off. They also can't reload  
it.*

I think that might be a good and necessary thing. It might annoy the users,  
but increased security often means reduced functionality. If the user can  
save changes to the profile, then so can a virus running as user. Some  
places specifically configure the profiles to be locked from being changed.  
Would it be acceptable to have the users get their profiles the way they  
want it, and then lock it down?

Are you sure the problem is with all rights [including execute] in the  
entire user profile [and not just certain files]? I would expect the main  
thing necessary is permissions on the ntuser\*. \* files in the root of the  
profile, and I would be surprised if execute was necessary. When  
troubleshooting ACL problems, I usually run filemon from  
[www.sysinternals.com](http://www.sysinternals.com) to find out what specific permission on which specific  
file is needed, does doing that help you reduce what permissions need to  
change, and could you just leave the permissions on those [presumably] few  
files in the default? That should still be just as secure, as long as you  
can leave the permissions on the default profile folder restricted.

> *First I created two scripts and stored them in  
> %systemroot%\system32\GroupPolicy\user\scripts\logon and ..\logoff  
> respectively. They were:  
>  
> logon.bat:  
> cscript %systemroot%\system32\xcaccls.vbs "%userprofile%" /T/E/Q/L/SPEC  
C  
> /P "%userdomain%\%username%":F  
> cscript %systemroot%\system32\xcaccls.vbs "%userprofile%" /T/E/Q/L/G  
> "%userdomain%\%username%":12345789ABCD*

microsoft.public.security: Re: [Updates] Re: More Before-The-Fact-Isms II

I would be afraid to depend on logon batch files executing as users for security. Logon scripts tend to fail or stop working from time to time and