

Re: Protecting assemblies from being used outside a company/group/team

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.security/2005-02/0043.html>

From: William Stacey [MVP] (staceywREMOVE_at_mvps.org)

Date: 02/02/05

Date: Wed, 2 Feb 2005 17:58:24 -0500

- > Unfortunately, it will be possible for code with adequate CAS permissions to
- > spoof this at runtime without decompiling your code if you use the .NET
- > framework methods for reading the strong name from the assembly. (This is
- > also one of the mechanisms used to spoof a StrongNameIdentityPermission
- > verification, so it's not exactly obscure.)

Thanks Nicole. Not sure I follow that completely. How does reading the strong name from the assembly help?

- > In addition, since your
- > obfuscated code will be calling into unobfuscated framework or CLR code, it
- > would be trivial to find the verification method in your assembly's IL, so
- > reverse engineering won't be nearly as difficult as you might hope.

You could find the logic points, but to create a "cracked" assembly and distribute you still need to make a change to the code and round trip the IL, which you can't do currently when using some obfuscators. Unless maybe I am not understanding this point (which is likely.) TIA

--

William Stacey, MVP

<http://mvp.support.microsoft.com>