

Re: Impersonation/Delegation security considerations

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2003-08/0363.html>

From: Rich (*rich_at_dha.net*)

Date: 08/27/03

Date: Wed, 27 Aug 2003 08:49:41 -0700

Hi Alek,

Your assumption and illustration of machines A, B, and C was 100% correct. Thank you very much for the internal security risk example. I will forward this info on to our network folks.

>-----Original Message-----

>Hi Rich,

>

>Our AD/network guys illustrated a potential security issue using the

>following example. By the way, I assume that by delegation you mean passing

>user's credential from one machine to the other, which would allow a Web

>application running on machine A to connect to a SQL server running on

>machine B using integrated Windows authentication with credentials

>(actually, authentication token or Kerberos ticket) of a remote user

>accessing the site from machine C. Without delegation, a Web application can

>only pass user's credentials to a SQL Server running on the same machine.

>So, let's say that I am an internal hacker and I would like to connect to

>some secure database using credentials of the company's CEO (CIO, or

>whatever). If delegation is enabled on my network, what I can do is:

>

>(1) Create a fake internal Web site.

>(2) *Send an HTML e-mail (or regular e-mail with a link) pointing to my fake Web site to the CEO (CIO, or whatever).*

>(3) *In the code-behind logic, use caller's credentials (Kerberos ticket) to connect to the database and do whatever I want on behalf of the user.*

>

>*The main danger in this scenario is that the user will never know what have happened. Without delegation, this risk is eliminated because my fake Web site would not be able to propagate user's credentials to the remote SQL Server unless I use basic authentication for the Web site, which is also a risk, but at least it will be visible to the user that some security-related operation is happening.*

>

>*Alek*

>

>*"Rich" <rich@dha.net> wrote in message news:008601c36b20\$50fc8dc0\$a301280a@phx.gbl...>> I'm having trouble finding specific documentation regarding the negative impact of using delegation in a Windows 2000 environment. I've read through numerous articles on using it, but if I do find anything that cautions the use of it, it reads like the following:*

>>

>> *Important:Delegation is a very powerful feature and is unconstrained on Windows 2000. It should be used with caution. Computers that are configured to support delegation should be under controlled access to prevent misuse of this feature.*

>>

>> *Our Network/Server side of the house does not want to implement delegation without knowing the immediate and potential security risks, and how to guard against them.*

>

>

>.

>