

Re: Basic security question

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2004-06/0194.html>

From: Ivan Brugiolo [MSFT] (ivanbrug_at_online.microsoft.com)

Date: 06/19/04

Date: Fri, 18 Jun 2004 19:36:05 -0700

> (e.g., why does "RegConnectRegistry()" succeed but then I can't retrieve
> values from the remote registry unless "WNetAddConnection2()" is called
> prior to "RegConnectRegistry()").

This seems the case of the "net use \\MachineName\IPC\$" first before using the remote resource if the RPC transport is over named pipe, and if the current SubjectContext does not have a suitable security context to negotiate authentication with the remote server.

"Programming Windows Security" from Keith Brown is good book.

--

This posting is provided "AS IS" with no warranties, and confers no rights. Use of any included script samples are subject to the terms specified at <http://www.microsoft.com/info/copyright.htm>

"Rob Bolton" <nospam@nospam.com> wrote in message news:eDzwYuZVEHA.2716@tk2msftngp13.phx.gbl...

> > It depends of the actual service you request on the remote machine, but
> most

> > often, the remote service that handles your request use impersonation,
> which

> > means it endorses your identity and credentials while working for you.
> This

> > way, all the security checks are made against your account.

> >

> > See ImpersonateLoggedOnUser, ImpersonateNamedPipeClient,
> > RPCImpersonateClient, RevertToSelf and related functions in MSDN for
> > details.

>

> Thanks very much to both you and Ivan. Just to clarify then, if a process on

> machine A makes a remote call to machine B via "RegConnectRegistry()" for
> example, two basic things typically happen:

>

> 1) Machine B first authenticates the identity associated with the thread
> that makes the call on machine A. This thread will usually be running
under

> the currently logged on user unless the thread is impersonating someone
else

> at the time. In either case, authentication will occur against the domain
> associated with that user (either machine A itself if the user is logged
in

> locally, the domain controller if the user is logged in against the domain

microsoft.public.platformsdk.security: Re: Basic security question

> controller, or possibly another workstation in the same or trusted domain).

> 2) Once authenticated, that user will then be impersonated on machine B so the standard Windows security model now kicks in. That is, the access token

> of anything that's executed on machine B will be the same as the thread that

> launched this on machine A in the first place (and checked against all DACLS

> on machine B as usual).

>

> I understand this is fairly simplistic and issues such as delegation and so

> forth can cloud the picture, but is this basically correct or am I way out

> in left-field? BTW, can either of you recommend a good book or white-paper

> on the subject (remote security in particular). The basic Windows security

> model is fairly straight-forward but remote issues like this are murky

> (e.g., why does "RegConnectRegistry()" succeed but then I can't retrieve

> values from the remote registry unless "WNetAddConnection2()" is called

> prior to "RegConnectRegistry()"). Thanks again.

>

>