

Re: CreateProcessAsUser "loses" privileges, why?

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2005-04/msg00683.htm>

- *From:* "Ivan Brugiolo [MSFT]" <ivanbrug@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 26 Apr 2005 01:36:59 -0700
-

As a rule of the thumb:
impersonation that happens via SSPI does not strip privileges (since it requires authentication first),
while impersonation that happens by the kernel trusting itself, does strip privileges
(since it does not require authentication).
The rationale being that across a network authentication hop privileges may mean nothing.

SSPI is the authentication process that uses
InitialzieSecurityContext/AcceptsSecurityContext/ImpersonateSecurityContext,
and it's used by RPC on top of other transports, by ISA, by
InternetExplorer/IIS4/5/6,
except rpc-over-LRPC, where LPC ports are used.

This may seem even more confusing, but,
you can cross check yourself via `!token` in KD.

--

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>

"Stefan Kuhr" <kustt110@xxxxxx> wrote in message
news:426DF791.3391102D@xxxxxxxxxx

> Hi Ivan,

>

> "Ivan Brugiolo [MSFT]" wrote:

>>

>> Is the SeDebugPrivilege enabled or not before the CreateProcessAsUser
call ?

>> You can use `!token <handle>` in a recent cdb/ntsd/windbg debugger to
see

>> that.

>>

>

> I placed the code that enables the SE_DEBUG_NAME privilege at the wrong

Re: CreateProcessAsUser "loses" privileges, why?

- > place in the client. Rats! It now works, the process created by CPAU
- > from the duplicated impersonation token has the SE_DEBUG_NAME privilege.
- > Just in case I ever wanted to replace this local named pipe connection
- > with an LRPC connection, would anything have to be changed? Again: are
- > the rules for stripping privileges from an impersonation token via the
- > different impersonation variants (ImpersonateNamedPipeClient,
- > RpcImpersonate, ...) documented anywhere?
- >
- > Thanks for your help, Ivan,
- >
- > --
- > Stefan Kuhr
- >
- > "Lesen schadet der Dummheit"

• Follow-Ups:

- ◆ [Re: CreateProcessAsUser "loses" privileges, why?](#)
◇ From: Stefan Kuhr

• References:

- ◆ [CreateProcessAsUser "loses" privileges, why?](#)
◇ From: Stefan Kuhr
- ◆ [Re: CreateProcessAsUser "loses" privileges, why?](#)
◇ From: Pavel Lebedinsky
- ◆ [Re: CreateProcessAsUser "loses" privileges, why?](#)
◇ From: Stefan Kuhr
- ◆ [Re: CreateProcessAsUser "loses" privileges, why?](#)
◇ From: Ivan Brugiolo [MSFT]
- ◆ [Re: CreateProcessAsUser "loses" privileges, why?](#)
◇ From: Stefan Kuhr
- ◆ [Re: CreateProcessAsUser "loses" privileges, why?](#)
◇ From: Stefan Kuhr
- ◆ [Re: CreateProcessAsUser "loses" privileges, why?](#)
◇ From: Ivan Brugiolo [MSFT]
- ◆ [Re: CreateProcessAsUser "loses" privileges, why?](#)
◇ From: Stefan Kuhr

- Prev by Date: [Re: How to control the exception handling of a child process?](#)
- Next by Date: [Re: Enable or disable devices](#)
- Previous by thread: [Re: CreateProcessAsUser "loses" privileges, why?](#)
- Next by thread: [Re: CreateProcessAsUser "loses" privileges, why?](#)
- Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)