

## Re: Remote process with network access

**Source:**

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.wmi/2004-09/0041.html>

---

**From:** chris delaney ([chrisdelaney\\_at\\_discussions.microsoft.com](mailto:chrisdelaney_at_discussions.microsoft.com))

**Date:** 09/04/04

Date: Sat, 4 Sep 2004 04:45:01 -0700

these are batch jobs that move files around. the machines are locked down properly and i would not want to compromise that.

the way i look at it, if i can provide a userid/pwd that is valid for the machine, i should be able to initiate a process on that machine to run code installed on that machine and it should all the rights as if i ran it interactively.

thx

"Ivan Brugiolo [MSFT]" wrote:

- > *The credentials of the account needs to be delegatable*
- > *and the machine account needs to be trusted for delegation.*
- >
- > *The only reason I can see for not structing for delegation a machine account*
- > *is that the machine is compromiseable, that is, it's easy to have arbitrary*
- > *code running as localsystem.*
- > *If you have code running as localsystem in a machine trusted for delegation,*
- > *then, if you can induce an authentication over it (for example,*
- > *by creating a web server and forcing a user to navigate that web server*
- > *with non anonymous credentials), then you can impersonate delegat-able*
- > *credentials,*
- > *and perform any action on behalf of the user.*
- >
- > *I guess that your scenario is a corporate network where users are allowed*
- > *to log-in as local administraotrs. In this case, delegation is dangerous.*
- >
- > --
- > *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/cpyright.htm>*
- >
- >
- > *"Gerry Hickman" <[gerry666uk@yahoo.co.uk](mailto:gerry666uk@yahoo.co.uk)> wrote in message*
- > *news:#Kj3xKHkEHA.2544@TK2MSFTNGP10.phx.gbl...*
- > > *Ivan Brugiolo [MSFT] wrote:*

> > > *The only authentication infrastrucutre that supports more than one hop*  
> *is*  
> > > *Kerberos.*  
> >  
> > *The problem with this (as I see it) is that Kerberos only works over two*  
> > *hops after you enable "Delegation" in Active Directory, and no one does*  
> > *enable it for security reasons. Even if you did enable it, is it not the*  
> > *case that you have to do this for EVERY remote machine you wanted to*  
> > *work with, or is it only the second hop machine that needs it?*  
> >  
> > *Either way, none of the above seems like a sensible option to me.*  
> >  
> > --  
> > *Gerry Hickman (London UK)*  
>  
>  
>