Re: Lightweight logon? Impersonation? − shared workstation problem

Source:
http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2008−06/msg00026.html

- *From*: "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxx>
- *Date*: Fri, 13 Jun 2008 22:14:41 −0500

I guess I still don't understand. If you are trying to access a website, the login to IIS is a network login which is processed nearly instantaneously. There are no login scripts executed.

Is this a web app or a local app you want to access?

Joe K.
−−
Joe Kaplan−MS MVP Directory Services Programming
Co−author of "The .NET Developer's Guide to Directory Services Programming"
http://www.directoryprogramming.net
−−
"THG" <THG@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:47A89A0D−DD8E−48C4−9BE9−004593550CCF@xxxxxxxxxxxxxxx

> Joe,
>
> The trick here is that login takes time and therefore your proposed approach
> seems to result in a lengthy logon. I am looking at the ways of allowing user
> access to a very limited set of resources on the network, primarily on the
> web server for a single application, under their Windows identity, on top of
> a generic user account that logs the workstation on. For that, I would not
> want them to go through all the logon scripts and all the Windows updates
> that might be part of the logon process. I want them to switch context while
> they are in the application in a couple seconds, upon entering their login ID
> and password. For that, impersonation seems to be a better tool. I hope I am
> I explaining my problem clearly.
>
> Tamara
>
> "Joe Kaplan" wrote:

Basically, if you disable automatic login with Windows Integrated Auth in the browser, the web app will just challenge the user for credentials and force them to log in. The login they provide to the server will then not be
coupled to the identity of the login on the workstation itself.

You don't need any impersonation or delegation to make this work, but you could definitely impersonate the end user in the app if you wanted to and could delegate if you wanted to as well.

You do need to do something to make sure the browser window is not reused by
something else. Closing it is ideal. :)

Joe K.
−−
Joe Kaplan−MS MVP Directory Services Programming
Co−author of "The .NET Developer's Guide to Directory Services Programming"
http://www.directoryprogramming.net
−−
"THG" <THG@xxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:8E838D97−2143−48A5−BDB6−63679E773FFC@xxxxxxxxxxxxxxx

> Joe,
>
> Thank you for replying. Would disabling automatic
> integrated
> authentication
> mean that users will not have to go through a complete logon
> and
> workstation
> can be logged on a basic generic account? Our problem is
> that users
> might
> not have enough discipline to close the browser when they
> are done with
> the
> session, so we might have to look into closing the browser
> window for
> them
> at
> a certain time in the transaction.
>
> As for smart cards, we don't have them and the proposed
> solution above
> seems
> to be overly complicated, so I would use it as a last resort.

Could any kind of impersonation/delegation be used on the application
level
on the server?

"Joe Kaplan" wrote:

> Can you disable automatic integrated authentication in IE for the
> machines
> in question so that the users will simply be prompted to enter
> credentials
> when they access the app? Then, have them close the browser when they
> are
> done.
>
> If you have smart cards, you could also just use SSL with client cert
> auth.
> The user would need to enter their smart card and PIN to log in.
>
> Joe K.
> −−
> Joe Kaplan−MS MVP Directory Services Programming
> Co−author of "The .NET Developer's Guide to Directory Services
> Programming"
> http://www.directoryprogramming.net
> −−

.