

Delegation in ASP.NET

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2004-09/0165.html>

From: matthewt (*matthewt_at_nospam.nospam*)

Date: 09/13/04

Date: Mon, 13 Sep 2004 07:11:01 -0700

Hi,

As the title suggests I have a question about delegation in ASP.NET.

We have an ASP.NET application running on a web server which requires clients to authenticate via Windows Integrated authentication. We're running in a Win2K native-mode domain and the clients are IE6 so we should be using Kerberos to authenticate.

At some points the application needs to send an email on behalf of the client; this it achieves by impersonating the remote user and using WebDAV to talk to the exchange server running on the DC (which is a physically separate box from the web server).

This is working in the main and the credentials appear to flow from the browser, through the web-app to the exchange server.

However, it only hangs together with a certain set of *browser* settings :

If the site is configured to live in a zone (e.g. Intranet or Trusted Sites etc.) that has either of the "automatic logon..." options in the IE custom security level dialog selected then all is well.

As soon as this isn't true and we manually enter the credentials when prompted, we authenticate with the web-server OK, but then the ASP.NET app can't authenticate with the exchange box on the client's behalf (its as if we're back to impersonation rather than delegation).

We believe that we've all the accounts are correctly configured for delegation (i.e. user accounts are *not* marked as sensitive, app account is marked as trusted for delegation, machine account trusted for delegation).

Does anyone have any ideas about what this browser option is actually doing that makes the whole thing work?

The application only supports windows integrated authentication so it can't be "falling back" to basic – is it falling back to NTLM though?

Any help will be much appreciated.

cheers,
Matt