

Re: Need for encryption in WSE 3.0 if using SS-avoid man-in-middle

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2006-10/msg00129.html>

- *From:* John K <KTJ@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 20 Oct 2006 12:24:02 -0700
-

The part that is confusing for me is the fact that we are allowing the user to change the URL. Thus, correct me if I am wrong, in this scenario; in order to detect we are connected to the wrong server (even though its SSL certificate is OK and valid by Verisign); we would need a client certificate. Correct? If so, as I asked in a few messages, how do I generate a client certificate? Can I generate a matching client certificate from the server's SSL certificate OR do I need another set of certificates (a client and server)? Are there any articles that go into detail on how to verify you are talking to the right server. Again, in my case my customer may host the server application; thus when I write the client S/W; I have no idea as to what server is valid. It sounds like verifying the public certificate at the client end matches the server certificate is the way to go. Do you have any tips to what to look for in the certificate's attributes in this scenario? Do I simply verify my client certificate is the public version of the server's certificate and thus that means I am talking to the right server? Thus, the customer could simply just place the public version of the server's certificate in our client application directory? Thanks alot. I am new to this and just want to make sure I have a secure application.

--

Thank you.

"Steven Cheng[MSFT]" wrote:

Hi John,

Yes, your concern that some malicious user may redirect the user to a fake server is reasonable. However, this can be detected by SSL/HTTPS client in almost every webclient implementation. For example, in IE browser, when you visit a ssl/https protected site, if the server certificate is not in your client machine's trust storage, IE will raise dialog to alert you and only if you proof to continue will the https/ssl connection successfully establish.

When you use .net network API(such as webservice proxy or webrequest class) to access remote SSL/https service, there also exist programming interface

Re: Need for encryption in WSE 3.0 if using SS–avoid man–in–middle

to do the validation. I've mentioned the "ServicePointManager.ServerCertificateValidationCallback" event in my first reply, is there any particular reason or difficulty that this is not suitable in your scenario?

This event is firing everytime at the initialize time of a https/ssl connection between client and server(when the client just receive server's SSL certificate), you can query the certificate's attributes to determine whether it is your expected one(this validation logic is up to you since you know what certificate is expected). Surely, at that time, the webservice hasn't send any message since SSL/HTTPS connection is even not established, if you found that the server certificate is not expected one, just return false for the function or even through exception.

Here is my original message in first reply

=====

If your concern is that some malicious one else may redirect the request to a fake server with SSL/certificates, then you can add codelogic in your client application to valiate the server certificate exposed from the SSL/HTTPS server. The ServicePointManager class in .net framework provide ServerCertificateValidationCallback event that can let us add custom code logic to verify the server (which provide the SSL/HTTPS service hannel). And this event will occur at the initial time when your webservice (or other webclient) which connect to HTTPS/SSL server through .net webrequest components:

#ServicePointManager.ServerCertificateValidationCallback Property
<http://msdn2.microsoft.com/en-us/library/system.net.servicepointmanager.servercertificatevalidationcallback.aspx>

#RemoteCertificateValidationCallback Delegate
<http://msdn2.microsoft.com/en-us/library/system.net.security.remotecertificatevalidationcallback.aspx>

=====

Anyway, I think https/ssl the preferred approach if possible since it is much simpler and strong for secure channel over http.

Sincerely,

Steven Cheng

Microsoft MSDN Online Support Lead

This posting is provided "AS IS" with no warranties, and confers no rights.

Re: Need for encryption in WSE 3.0 if using SS—avoid man—in—middle