

Re: SSL/TLS & renegotiation and Internet Explorer

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-07/msg00071.html>

- *From:* "John Banes" <jabanes@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 5 Jul 2006 16:16:43 -0700
-

I've looked at the behavior of IE in detail a number of times over the years. Here are my recollections.

When IE closes the connection with the server and prompts the user to choose his digital certificate, it also releases its handle to the SSL context. The underlying SSL implementation that IE uses (schannel) doesn't expect applications to do this in the middle of a handshake, and so as part of its recovery logic the SSL session is discarded. This means that the new connection that IE establishes after the user chooses a client certificate will not resume the original session, but instead a brand new session will be created. That is, the ClientHello message will contain a brand-new session id. I can think of no way to reliably associate the new session with the original one. I've long considered this to be a bug in IE.

If the user only has one suitable client certificate, then recent versions of IE can be configured to send the client certificate without prompting the user. When this is done, the connection is not closed and no new session is artificially created. This should work better from your perspective.

I'm not sure how IE7 behaves...

Regards,
John

"Suresh Chandra" <SureshChandra@xxxxxxxxxxxxxxxxxxxxxx> wrote in message news:20350D8A-A161-4266-8C23-B49F7069596A@xxxxxxxxxxxxxxxxxxxxxx

Dear All,

I am working on my own server that supports SSL, both with and without client authentication. I am in the process of implementing a feature which allows the server to prompt the user to provide his digital certificate whenever he tries to access a resource that requires client authentication.

So whenever i get a request for such a Page then my server sends a SSL HelloRequest to the Client thus initiating a SSL renegotiation. The server caches the HTTP request in its Session buffer before it initiates the renegotiation.

Re: SSL/TLS & renegotiation and Internet Explorer

So, the client re-initiates the handshake by sending the 'client-hello' packet (encrypted with the session key negotiated in the previous session) and the server reciprocates with the serverhello, server cert, client cert request and server hello done packets, all encrypted with the older session key.

At this stage, IE closes the connection with the server and prompts the client to choose his digital certificate. When the client chooses the certificate it re-initiates the handshake, establishes a new connection and then starts the handshake process again with the 'client-hello' packet.

Now, at this stage I am not sure how to link up the old SSL session and the new SSL session on the server side. Actually I have to forward the HTTP request to another backend server, get the response and forward it to the IE client.

My question is how do i link the old and new sessions that i have established with the Internet Explorer. Is there anything that will be common between the two sessions

Any help on this would be greatly appreciated.

Regards