

Re: SSL without certificates

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2003-07/0079.html>

From: Terry (terry_at_hotmail.com)

Date: 07/05/03

Date: Sat, 5 Jul 2003 12:59:46 +0800

Quote: mccarthur@btinternet.com wrote that the client needs the server's cert

because the client uses the public key from the cert to encrypt the data sent to the server. That is not correct. The data sent back and forth along the SSL connection are encrypted using a symmetric (secret) key, not a public key. The secret key is created during the SSL handshake.

As far as I know, in a SSL connection, the server's cert sent to client is used to encrypt the session key(secret symmetric key) generated on the client side which is then sent to the server for use in the connection. So if the you dont use a server's cert, how can this be done?

"MS" <ms@ms.net> wrote in message news:3F05AC99.5040000@ms.net...

> *Splatter wrote:*

> > *"MS" <ms@ms.net> wrote in message news:3F0428C6.5020609@ms.net...*

> >

> > > *I want to use SSL for client to server communication. The server is*

> > > *W2K. I don't care about server authentication, I just want to*

> > > *encrypt the connection. Do I still have to create and install a*

> > > *dummy certificate for the server, or is there a way to bypass it?*

> >

> >

> > *I'm not sure what your specific needs are but I got around this using*

> > *2K at home by installing the windows certificate authority, and using*

> > *it to roll my own CA & website certificate. HTH DP*

> >

> >

>

> *In response to my question (the post attached above) I got a lot of*

> *advice and information from Splatter and others. But I still don't know*

> *the answer to my original question:*

>

> *Does the Microsoft W2K implementation of SSL=TLS allow bypassing the*

> *handshake step that sends server's certificate to the client? In other*

> *words, can I set up an SSL-encrypted connections to the W2K server*

> *without installing a certificate on the server?*

>

> *The specification of the TLS standard does allow that: The handshake*

alt.computer.security: Re: SSL without certificates

- > *protocol can be set up so that no certificates are used, and the client*
- > *and the server use an "anonymous" key exchange protocol to agree on an*
- > *encryption key. The question is, does Microsoft implementation allow it?*
- > *And if so, how do I configure the server to operate this way?*
- >
- > *As I said in my original post, I want to use SSL to encrypt the*
- > *client-to-server connections. So the advice to use SSH or IPSec doesn't*
- > *help.*
- >
- > *My client is not a browser, so I am not worried about any popup messages*
- > *that specific browsers may display when they cannot authenticate a web*
- > *server.*
- >
- > *mccarthur@btinternet.com wrote that the client needs the server's cert*
- > *because the client uses the public key from the cert to encrypt the data*
- > *sent to the server. That is not correct. The data sent back and forth*
- > *along the SSL connection are encrypted using a symmetric (secret) key,*
- > *not a public key. The secret key is created during the SSL handshake.*
- >
- > *Rainer Gerhards wrote that I can get a free certificate from sources on*
- > *the Internet. That's good information, but I would prefer not to deal*
- > *with the cert at all if I can avoid it.*
- >
- > *ASMdood wrote that encryption without authentication is useless. I*
- > *agree, but in my application this is not an issue.*
- >
- > *As I stated in my original post, I cannot find the answers in Microsoft*
- > *documentation. Anybody out there who is familiar with the Microsoft*
- > *implementation of SSL in W2K and can answer my question?*
- >
- > *MS*
- >