

Re: which security protocol for dealing with this situation

Re: which security protocol for dealing with this situation

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-09/msg00036.html>

- *From:* comphelp@xxxxxxxxxx (Todd H.)
 - *Date:* 27 Sep 2007 17:48:26 -0500
-

ben@xxxxxxxxxxxxxxxx writes:

On Sep 27, 10:48 pm, comphelp@xxxxxxxxxx (Todd H.) wrote:

ssh would provide for these requirements. The ssh server has a host key that a proper ssh client will ask to verify upon initial connection, and will store for later connections, warning you if the host key changes.

Hmm, I was recently looking into a ssh connection for a shopping cart web site as ssh was essential for that if taking credit card numbers directly. Didn't do it in the end but for that it seemed a 3rd party certificate server was needed at a subscription cost per year.

Is it possible you're confusing SSL (secure sockets layer, synonymous colloquially with https:// and securing website traffic in transit) and ssh (secure shell)

And the IP address of the merchant's server had to be static. But I've just read about ssh in a security book which I'm reading at the moment (Computer Security 2ed Dieter Gollman) and what was in that book didn't really tally with what I found out when I was looking into implementing a shopping cart web site -- in particular the 3rd party certificate server part wasn't mentioned at all in the book for ssh I don't think, so I'm not sure what's going on there entirely.

SSH doesn't use third party certificates, certificate authorities or what not. ssh-keygen creates its own key and the whole sticky wicket

Re: which security protocol for dealing with this situation

Re: which security protocol for dealing with this situation

of verification is left up to the individual user. No trusted cert authorities are employed.

However, given requirements that you illuminated in another post (i.e. you can't install any software on your clients), SSH ceases to be a usable solution. To use SSH, you'd need an SSH enabled client program.

Forgetting online store web servers, for what I'm asking about would a 3rd party certificate server therefore subscription be necessary?

It depends.

Would like to avoid anything like that if possible.

Okay, if your clients only have web browsers available, and if you don't want base computer owners to pay any sort of certificate fee, your best option is probably going to be creating self signed SSL certificates, but... the verification of whether the client trusts to connect to the server will be handled by the web browser in the mobile device, not anything under your control.

So, to be really sure, a diligent user would have to scrutinize the self signed certificate (and the web browser should prompt the user with a warning when it encounters SSL certificates that aren't signed by a certificate authority the browser trusts), and the user could contact the base computer owner independently to verify its authenticity. But such diligent users are quite an exception.

There may be other ideas out there. I'm not a crypto and certificate expert by any stretch.

Best Regards,

--

Todd H.

<http://www.toddh.net/>

.