
concerns about SSL and the iSDK

Posted by nonickch - 2009/10/16 01:45

Another issue that is lately bugging me:

Why is the iSDK setting:
`setSSLVerifyPeer(FALSE);`

Our communication does get encrypted, meaning noone can listen in on the contact/CC info being passed by, but noone can stop somebody residing anywhere between our script and the infusion server performing a Man-in-the-middle attack

For people unaware of MITM attacks and don't care to read the link (you should), it pretty simple:
Someone intercepts the communication and pretends to be the infusionsoft server. He accepts our requests, saves a copy, then forwards them to the real infusionsoft server. Then receives the reply and forwards it back to us.

SSL provides both encryption and authentication, and by dropping `SSLVerifyPeer` we effectively drop the authentication part rendering encryption next to useless (anyone that can listen in on the communication can also perform MITM).

=====