

Re: basic ssl proxy question

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-06/0344.html>

From: Fred Holm (*dontreplyviail_at_hotmail.com.invalid*)

Date: 06/22/03

Date: 22 Jun 2003 02:13:51 +0200

First of all, many thanks for answering. But I must confess, I am confused by your article... ;-) You seem to contradict yourself sometimes, or I misunderstand completely.

"Bjorn Randell" <Bjorn@AlphaMale.me.uk> wrote:

>> *In the past, I had thought, using an ssl proxy for a program which normally is used without proxy would ensure encryption and anonymity, but maybe, this is complete nonsense, right?*

>

>*In this case, encryption is only between you and the proxy. Any access which the proxy sends to the outside world will be unencrypted and suseptable to classic sniffing techniques.*

Let's tag your statement above and call it A1. ;-)

Between the ssl proxy and the peers on the other end of the world: no encryption; all right, that's what I suspected, too.

Between me and the ssl proxy: according to your statement A1 there IS encryption – that's what I still don't know for sure.

>> *Does involving such an ssl (connect) proxy mean, the traffic from my computer to the ssl proxy is encrypted? Does it even mean, the traffic*

>> *from the ssl proxy to the p2p partner at the other end is encrypted?*

>

>*1.) The method used to get out to IPs on different ports is achieved*

>*using*

>*the SSL CONNECT command, which, AFAIK, involves no encryption*

>*whatsoever!*

>*(Use a packet sniffer for complete verification on this one, I'm 99%*

>*sure*

>*though that there is no encryption.)*

Let's call your statement A2.

Here, you claim, again, that there is no encryption to the different IPs on different ports on the other side of the file sharing process.

So, you don't say anything different from A1 and I can follow you.

Or do I misunderstand, did you talk about "no encryption between me and the ssl proxy" here? (which would contradict A1)

>2.) *Even if I'm wrong, and it does encrypt the traffic between your
>socks
>server and the proxy, it certainly can't encrypt between the proxy and
>the
>P2P partner your downloading/uploading from/to.*

And let's tag this B1

Here, I really can't follow you, because you highly doubt, there is encryption between my socks proxy and the ssl proxy ("even if I'm wrong..." etc.). This is in clear contrast to A1, isn't it, where you claim, there IS encryption between me and the chosen ssl proxy?

>> *Or does it mean, there is no encryption at all!? Because the so
>> called
>> ssl proxy only passes my requests through – and since there are no
>> (browser, or whatever) certificates/public keys exchanged, there
>> CANNOT
>> be any kind of encryption or anonymity?
>
>We've establish now that no encryption happens, however, there is a
>little
>more anonymity. That comes from the fact that anyone you download from
>is
>only going to see the IP address of the proxy which is connected to
>them,*

Let's call your statement C1 now.

And I am puzzled. You say, "we've established now that no encryption happens"! Why? Above (in A1) you said, there IS encryption – not between ssl proxy and the rest of the world, BUT between me and the ssl proxy.

Why then do you state here, there is no encryption at all? Or do I misunderstand your sentence, are you just talking again about the situation between ssl proxy and the rest of the world?

>> *And now, let's forget the socks proxies, because there are also
>> programs, like icq applications, which can directly use an ssl proxy
>> (without socksifying the icq application first).
>>
>> What happens in this case? If I use icq or some other program with an
>> ssl proxy, does encryption happen then or not?
>
>I'm pretty sure it's the standard SSL CONNECT command used to access
>AOL/ICQ
>servers, therefore it will be unencrypted between your ICQ client and
>the*

>proxy.

Your statement D1 :)

And it contradicts A1, though the situation is more or less identical to A1, isn't it?

>> *And finally, I hope, I am not wrong in this last scenario:*
>> *When using stunnel between my computer and an external shell account*
>> *and*
>> *using certificates, is my connection encrypted then?*
>> *Is this comparable to using secure shell tunneling?*
>
>*I just looked up some stunnel stuff and yeah, it's encrypted. I would*
>*however say, that if you are using stunnel just to connect to a shell*
>*on*
>*your shell provider, that you consider using SSH which is IMO a much*
>*better*
>*tool to use for the job. It's also more flexible from what I can*
>*gather and*
>*you can negotiate with the server over how you want data encrypted*
>*etc. AES*
>*is far more secure than what SSL has to offer.*
>
>*Anyway, the reason it gets encrypted using the stunnel method is that*
>*there*
>*is certificate exchange using the SSL protocol in the normal sense, and*
>*then*
>*data is exchanged. With the ICQ or other application that can use a*
>*proxy*
>*to get out, it uses the SSL CONNECT method to bounce out, which doesn't*
>*involve certificate exchange, it just allows 'port forwarding'*
>*facilities of*
>*a sort.*

So, if there is no certificate exchange, there can't be encryption, right?

If I use stunnel or the ssh tunneling capabilities or the web browser's certificate exchanging capabilities, there IS encryption, okay?

But if I just use an ssl proxy for a file sharing program, for icq, for access to a news server etc., there is NO encryption, because the ssl proxy behaves just like a normal (non ssl) proxy here, is this correct?

>> *Could someone with a deeper knowledge of all this enlighten me? I am*
>> *lost here and tend to think, I believed in illusions of encryption*
>> *and*
>> *anonymity regarding ssl proxies...*
>
>*This is kinda one of my topics of interest, so if you've got anymore*
>*questions, shoot! :)*

comp.security.misc: Re: basic ssl proxy question

That's what I did. :) I hope, you didn't get annoyed by my critical analysis of your argumentation... Perhaps, I understood things differently from what you meant to express...

Would be fine, if you could elaborate somewhat more on this. And of course, other opinions (from more people) – or rather – not opinions, but FACTS, are welcome as well.

Thanks again
Fred