

## Re: SSL Overhead?

**Source:**

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.compactframework/2004-08/1429.htm>

---

**From:** Rick Winscot (*rickly\_at\_zyche*)

**Date:** 08/24/04

Date: Tue, 24 Aug 2004 13:39:21 -0600

Eugene,

Lets talk security.... A simple TCP service will allow you to run on a minimal windows install... which means you can bypass the need to be running a web server. Keep in mind that IIS is a highly targeted system – prone to attack, exploits and can become a front door into your system. Your system is only as strong as the weakest link... and while web services tout 128 bit encryption – this is useless if there is a backdoor wide open. Not to mention the fact that SSL has security issues as well. Please don't follow with a one line quip to the effect of "what are you talking about." If you are worth your salt, you will be well aware of the specific security issues that surfaced in 2000 as well as the general issues that continue to plague SSL systems.

In order to guarantee security, it is wise to reduce the subset of software running on the machine... the fewer the better. I find it comical to hear people talk about security as an absolute... there is no such thing as a 100% secure system. In fact – your security should be directly proportional to the value of the data that you are sending.

I'd like to challenge your issue of security... and add to it economy of exchanged data. Also – in answer of your question on what algorithm causes data expansion in ssl... I have to say this. All encryption methods cause some data expansion. This can be counteracted by pre or post compression but for small bits of data... is ineffectual. Data expansion in encryption is a constant.

Per the users original question. SSL will add additional overhead and further lengthen the time the GPRS connection is active... this is a given. SSL is slower... a lot slower than straight HTTP and for these small bits of data... will more than likely double the phone bill.

Cheers,

Rick Winscot  
www.zyche.com

"Eugene Mayevski" <mayevski@eldos.org> wrote in message  
news:ejSHSheiEHA.1652@TK2MSFTNGP09.phx.gbl...

> *Hello!*

> *You wrote on Tue, 24 Aug 2004 00:50:55 -0600:*

>

> *RW> I haven't heard of a case where encryption actually makes the data*

> *RW> smaller... unless you are using a real simple XOR routine that is*

> *RW> character for character... in any case the smallest that you can go*

*is*

> *RW> 1 : 1 if you don't use compression, even then there are limits to how*

> *RW> small the data can be compressed – – encryption does come into the  
mix.*

> *RW> SSL \*can\* and \*may\* double the size of each packet you send.*

>

> *Examples please? Which algorithm (from the ones used in SSL) will double  
the*

> *size of Web Service request?*

>

> *RW> Next... give this a try. Try using regular TCP to send the data.*

*Since*

> *RW> the data is already secure... webservices may be holding you back. I*

> *RW> have a sample CF TCP wrapper that I would be happy to send... you may*

> *RW> find that the bulk of a web service is unnecessary and far more  
costly*

> *RW> than just send the data directly. I can think of a hundred reasons  
why*

> *RW> a simple home-made protocol will end up saving you lots of money, a*

> *RW> huge headache, a ton of testing, and give you a better (more  
reliable)*

> *RW> product. Let me know if you would like to do a performance*

> *RW> comparison...*

>

> *And be as insecure as one can't even imagine ...*

>

> *With best regards,*

> *Eugene Mayevski*

>