Ruby master - Bug #9822

Ruby doesn't respect system OpenSSL configuration

05/09/2014 09:24 PM - Envek (Andrey Novikov)

Status:	Closed		
Priority:	Normal		
Assignee:	openssl		
Target version:			
ruby -v:	ruby 2.2.0dev (2014-05-10 trunk 45893) [x86_64-linux]	**Backport:**	2.0.0: REQUIRED, 2.1: REQUIRED

Description

Hello.

I need to work with SSL (HTTPS) with GOST encryption, but ruby doesn't connect to the servers that requires GOST algorithms to be used for encryption.

The issue is in fact, that it is required to modify system OpenSSL config to GOST work properly (see GOST engine README in OpenSSL source: https://github.com/openssl/openssl/blob/master/engines/ccgost/README.gost)

If system OpenSSL correctly configured, openssl tools works fine (e.g. openssl s_client will connect).

But even the system with OpenSSL configured ruby would not connect to the GOST HTTPS servers.

Solution

After some googling I've found post from people who have patched PHP to work with GOST HTTPS, and I've tried to make the similar patch for Ruby. There is also info, that other software like curl also needs such a patching. (Post (in russian): http://habrahabr.ru/post/189352/)

And it works!

Patch is attached to this issue. I've tested it with 2.1.1 and today trunk in Ubuntu Linux 12.04 and Mac OS X 10.9 (both with RVM).

How to test

Upgrade and configure your OpenSSL (you need version 1.0.0 or above), instructions for configuring and testing can be found in links above.

Try to execute attached ssl_example.rb script (it effectively downloads root page of https://ssl-gost.envek.name/ site, that I've configured for this, be aware that usual browsers won't be able to connect to it and only Firefox will display useful error message)

You should get some text with SSL connection info to STDOUT if it works and exception otherwise.

Another server for test: https://service.rosminzdrav.ru/

Workarounds

For HTTPS with GOST I've written a little gem that wrapping openssl s_client utility:
https://github.com/Envek/httpi-adapter-openssl_gost

History

#1 - 05/09/2014 10:02 PM - zzak (Zachary Scott)

- Status changed from Open to Assigned

#2 - 06/19/2014 01:36 PM - Envek (Andrey Novikov)

Can anyone review this? Patch is very simple (one line!).

Also, there is related issue: https://bugs.ruby-lang.org/issues/9830

#3 - 06/23/2014 11:04 PM - zzak (Zachary Scott)

- Target version set to 2.2.0

#4 - 09/13/2015 03:10 AM - zzak (Zachary Scott)

- Assignee changed from MartinBosslet (Martin Bosslet) to openssl

#5 - 11/17/2016 06:11 PM - wolfer (Sergey Fedosov)

much needed patch, I often used gost-crypt

#6 - 08/11/2019 06:23 PM - jeremyevans0 (Jeremy Evans)

I submitted a pull request to ruby-openssl to use OPENSSL_config: https://github.com/ruby/openssl/pull/267

#7 - 10/08/2019 12:28 AM - jeremyevans0 (Jeremy Evans)

- Status changed from Assigned to Closed

After some research by ioquatix (Samuel Williams), OpenSSL 1.1.0+ should now work correctly and we should not need this setting. If this doesn't work for you with OpenSSL 1.1.0+, or you would like like Ruby to support older versions of OpenSSL with this feature, please reopen the pull request: https://github.com/ruby/openssl/pull/267

Files

respect_system_openssl_settings.patch	430 Bytes	05/09/2014	Envek (Andrey Novikov)
ssl_example.rb	558 Bytes	05/09/2014	Envek (Andrey Novikov)