Ruby master - Feature #4481

Add client_ca method to OpenSSL::SSLSocket

03/08/2011 02:56 AM - ohai (Ippei Obayashi)

Status:	Closed	
Priority:	Normal	
Assignee:	nahi (Hiroshi Nakamura)	
Target version:	2.0.0	

Description

=begin
Please add "client_ca" method to OpenSSL::SSLSocket to solve the following problem.

Problem:
If a SSL server decide to authenticate clients using client-certificates,
the server can send the list of client CAs to a client as a hint, and
the client can use the list to select an appropriate certificate.
But the current ruby's ext/openssl does not have the API to access the list.

Solution:
Add a wrapper function for SSL_get_client_CA_list.

Two patches (new method and test) are attached to this message.
=end

Associated revisions

Revision 1dcd4b32 - 06/30/2011 02:48 PM - emboss

- ext/openssl/ossl.c/.h: Added ossl_x509_name_sk2ary.
- ext/openssl/ossl.c: Replaced ossl_x509_ary2k by generic macro to simplify future conversions.
- ext/openssl/ossl_ssl.c: Implement SSLSocket#client_ca.
- test/openssl/test_ssl.rb: Add test for SSLSocket#client_ca. Thanks to Ippei Obayashi for providing the patch! [Ruby 1.9 - Feature #4481] [ruby-core:35461]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@32337 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 32337 - 06/30/2011 02:48 PM - emboss

- ext/openssl/ossl.c/.h: Added ossl_x509_name_sk2ary.
- ext/openssl/ossl.c: Replaced ossl_x509_ary2k by generic macro to simplify future conversions.
- ext/openssl/ossl_ssl.c: Implement SSLSocket#client_ca.
- test/openssl/test_ssl.rb: Add test for SSLSocket#client_ca. Thanks to Ippei Obayashi for providing the patch! [Ruby 1.9 - Feature #4481] [ruby-core:35461]

Revision 32337 - 06/30/2011 02:48 PM - emboss

- ext/openssl/ossl.c/.h: Added ossl_x509_name_sk2ary.
- ext/openssl/ossl.c: Replaced ossl_x509_ary2k by generic macro to simplify future conversions.
- ext/openssl/ossl_ssl.c: Implement SSLSocket#client_ca.
- test/openssl/test_ssl.rb: Add test for SSLSocket#client_ca. Thanks to Ippei Obayashi for providing the patch! [Ruby 1.9 - Feature #4481] [ruby-core:35461]

Revision 32337 - 06/30/2011 02:48 PM - emboss

- ext/openssl/ossl.c/.h: Added ossl_x509_name_sk2ary.
- ext/openssl/ossl.c: Replaced ossl_x509_ary2k by generic macro to simplify future conversions.
- ext/openssl/ossl_ssl.c: Implement SSLSocket#client_ca.
- test/openssl/test_ssl.rb: Add test for SSLSocket#client_ca. Thanks to Ippei Obayashi for providing the patch! [Ruby 1.9 - Feature #4481] [ruby-core:35461]

Revision 32337 - 06/30/2011 02:48 PM - emboss

- ext/openssl/ossl.c/.h: Added ossl_x509_name_sk2ary.

- ext/openssl/ossl.c: Replaced ossl_x509_ary2k by generic macro to simplify future conversions.
- ext/openssl/ossl_ssl.c: Implement SSLSocket#client_ca.
- test/openssl/test_ssl.rb: Add test for SSLSocket#client_ca. Thanks to Ippei Obayashi for providing the patch! [Ruby 1.9 - Feature #4481] [ruby-core:35461]

Revision 32337 - 06/30/2011 02:48 PM - emboss

- ext/openssl/ossl.c/.h: Added ossl_x509_name_sk2ary.
- ext/openssl/ossl.c: Replaced ossl_x509_ary2k by generic macro to simplify future conversions.
- ext/openssl/ossl_ssl.c: Implement SSLSocket#client_ca.
- test/openssl/test_ssl.rb: Add test for SSLSocket#client_ca. Thanks to Ippei Obayashi for providing the patch! [Ruby 1.9 - Feature #4481] [ruby-core:35461]

Revision 32337 - 06/30/2011 02:48 PM - emboss

- ext/openssl/ossl.c/.h: Added ossl_x509_name_sk2ary.
- ext/openssl/ossl.c: Replaced ossl_x509_ary2k by generic macro to simplify future conversions.
- ext/openssl/ossl_ssl.c: Implement SSLSocket#client_ca.
- test/openssl/test_ssl.rb: Add test for SSLSocket#client_ca. Thanks to Ippei Obayashi for providing the patch! [Ruby 1.9 - Feature #4481] [ruby-core:35461]

History

#1 - 06/09/2011 06:38 AM - MartinBosslet (Martin Bosslet)

- Assignee set to MartinBosslet (Martin Bosslet)

Thanks Ippei for submitting this - I will have a look at it!

Regards,
Martin

#2 - 06/09/2011 08:42 AM - MartinBosslet (Martin Bosslet)

- Status changed from Open to Assigned

#3 - 06/30/2011 11:48 PM - Anonymous

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r32337.
Ippei, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/openssl/ossl.c/.h: Added ossl_x509_name_sk2ary.
- ext/openssl/ossl.c: Replaced ossl_x509_ary2k by generic macro to simplify future conversions.
- ext/openssl/ossl_ssl.c: Implement SSLSocket#client_ca.
- test/openssl/test_ssl.rb: Add test for SSLSocket#client_ca. Thanks to Ippei Obayashi for providing the patch! [Ruby 1.9 - Feature #4481] [ruby-core:35461]

#4 - 07/01/2011 12:17 AM - MartinBosslet (Martin Bosslet)

- Category set to ext

- Status changed from Closed to Feedback

- Assignee changed from MartinBosslet (Martin Bosslet) to nahi (Hiroshi Nakamura)

Just added Ippei's patch. I took the liberty to add a sentence to RDoc pointing out that in contrast to SSLContext#client_ca=, where we set X509::Certificates, the newly added SSLSocket#client_ca will only return an array of X509::Names.

I looked at how this is used internally by OpenSSL and as it turns out this list seems neither to be checked nor used at all during the handshake except for sending the list to the client. This means that it would be perfectly possible to send any list of certificates to the client, no matter if they're actually trusted or not. As a consequence, this means that it is the programmer's duty to keep this list correct and meaningful with respect to the actually trusted X509::Certificates.

This made me wonder - wouldn't it be nicer to have the list pre-populated with the CA certificates of the underlying X509::Store that serves as the basis for client certificate validation to have a meaningful default setting? Should the need arise to have a custom setting (e.g. sending a filtered subset of the trusted CA's in specific situations), developers would still be able to do so by overriding the default list using SSLContext#client_ca= on

the server side.

Another thing I don't like too much is that since the list is not checked internally it would also be possible to send untrusted CAs to the client. Although this is not undermining the security it still makes no sense since a client using a certificate issued by an untrusted CA would ultimately get rejected anyway. But nevertheless, I'd feel better if we forbid such silly things right away. Since we only use SSL_CTX_add_client_CA(SSL_CTX *ctx, X509 *cacert) for feeding the client CA list in ext/openssl, it would be possible for us to actually verify that those CA certificates are

a) contained in the list of trusted CA certificates or
b) at least that they are trusted intermediate certificates whose certificate path leads up to a trusted root being among the trusted CAs.

Wouldn't this be better? Or am I overlooking anything?

What do you guys think? Should one or both of these features added to what we have right now? If you think so, I would open a new ticket so this one can be closed.

PS: (I'll add further tests once we concluded on the topic, I just added a very basic test for now).

#5 - 07/10/2011 03:38 PM - naruse (Yui NARUSE)

- Target version changed from 1.9.3 to 2.0.0

#6 - 09/06/2011 09:37 PM - Anonymous

- Status changed from Feedback to Closed

This issue was solved with changeset r32337.
Ippei, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/openssl/ossl.c/.h: Added ossl_x509_name_sk2ary.
- ext/openssl/ossl.c: Replaced ossl_x509_ary2k by generic macro to simplify future conversions.
- ext/openssl/ossl_ssl.c: Implement SSLSocket#client_ca.
- test/openssl/test_ssl.rb: Add test for SSLSocket#client_ca. Thanks to Ippei Obayashi for providing the patch! [Ruby 1.9 - Feature #4481] [ruby-core:35461]

Files

ssl_client_ca.diff	2.12 KB	03/08/2011	ohai (Ippei Obayashi)
ssl_client_ca_test.diff	1.07 KB	03/08/2011	ohai (Ippei Obayashi)