Support for the ALPN TLS extension

ALPN [1] is a successor [2] to NPN, support for which was added in 2.0.0 [3]. HTTP/2 [4] is using ALPN to negotiate protocol support, and the spec is moving fast -- it'd be great to have ALPN support in one of the upcoming Ruby releases. Current status of ALPN support in various TLS libraries and languages:

https://github.com/http2/http2-spec/wiki/ALPN-Status

As a side note, for anyone interested, I have an implementation of draft-06 http/2 spec: https://github.com/igrigorik/http-2

[2] https://www.imperialviolet.org/2013/03/20/alpn.html

Associated revisions

Revision bc6e55c0 - 07/22/2015 06:31 PM - tenderlove

- ext/openssl/ssl_ssl.c: add ALPN support. [Feature #9390]
- ext/openssl/extconf.rb: detect ALPN support in OpenSSL
- test/openssl/test_ssl.rb: test for ALPN

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@51347 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 51347 - 07/22/2015 06:31 PM - tenderlovemaking (Aaron Patterson)

- ext/openssl/ssl_ssl.c: add ALPN support. [Feature #9390]
- ext/openssl/extconf.rb: detect ALPN support in OpenSSL
- test/openssl/test_ssl.rb: test for ALPN

Revision 51347 - 07/22/2015 06:31 PM - tenderlove

- ext/openssl/ssl_ssl.c: add ALPN support. [Feature #9390]
- ext/openssl/extconf.rb: detect ALPN support in OpenSSL
- test/openssl/test_ssl.rb: test for ALPN

Revision 51347 - 07/22/2015 06:31 PM - tenderlove

- ext/openssl/ssl_ssl.c: add ALPN support. [Feature #9390]
- ext/openssl/extconf.rb: detect ALPN support in OpenSSL
- test/openssl/test_ssl.rb: test for ALPN
ext/openssl/ossl_ssl.c: add ALPN support. [Feature #9390]
ext/openssl/extconf.rb: detect ALPN support in OpenSSL
test/openssl/test_ssl.rb: test for ALPN

Revision 51347 - 07/22/2015 06:31 PM - tenderlove

ext/openssl/ossl_ssl.c: add ALPN support. [Feature #9390]
ext/openssl/extconf.rb: detect ALPN support in OpenSSL
test/openssl/test_ssl.rb: test for ALPN

Revision 51347 - 07/22/2015 06:31 PM - tenderlove

ext/openssl/ossl_ssl.c: add ALPN support. [Feature #9390]
ext/openssl/extconf.rb: detect ALPN support in OpenSSL
test/openssl/test_ssl.rb: test for ALPN

Revision edf712bf - 07/26/2015 10:21 AM - nobu (Nobuyoshi Nakada)

ossl_ssl.c: fix condition

Revision 51392 - 07/26/2015 10:21 AM - nobu (Nobuyoshi Nakada)

ossl_ssl.c: fix condition

Revision 51392 - 07/26/2015 10:21 AM - nobu (Nobuyoshi Nakada)

ossl_ssl.c: fix condition

Revision 51392 - 07/26/2015 10:21 AM - nobu (Nobuyoshi Nakada)

ossl_ssl.c: fix condition

Revision 51392 - 07/26/2015 10:21 AM - nobu (Nobuyoshi Nakada)

ossl_ssl.c: fix condition

History
#1 - 01/14/2014 01:16 AM - drbrain (Eric Hodel)

03/14/2022
- Status changed from Open to Assigned
- Assignee set to MartinBosslet (Martin Bosslet)

#2 - 08/04/2014 10:28 PM - cabo (Carsten Bormann)
Note that RFC 7301 has published:  http://tools.ietf.org/html/rfc7301
HTTP/2 is nearing completion and requires ALPN, so if Ruby wants to play in this space, ALPN needs to be done with high priority now.

#3 - 11/29/2014 09:42 PM - igrigorik (Ilya Grigorik)
Carsten Bormann wrote:

Note that RFC 7301 has published:  http://tools.ietf.org/html/rfc7301
HTTP/2 is nearing completion and requires ALPN, so if Ruby wants to play in this space, ALPN needs to be done with high priority now.

+1. Anything we can do to move this forward?

#4 - 11/29/2014 10:08 PM - normalperson (Eric Wong)
ilya@igvita.com wrote:

+1. Anything we can do to move this forward?

A patch and test cases would be nice.
I'm mildly interested in this, too, but don't trust myself with OpenSSL.

#5 - 12/24/2014 10:48 PM - normalperson (Eric Wong)
Note: ALPN requires OpenSSL 1.0.2, which is only in beta3 as of now (2014/12/24). I suspect few are willing to use a beta version of OpenSSL on their servers. But I look forward to this feature.

#6 - 02/07/2015 02:03 AM - tbetbetbe (Tim Emiola)
FYI: ALPN support landed in the recent 1.0.2 version release of openssl.

#7 - 07/15/2015 02:07 AM - tendervlove (Aaron Patterson)
- File 0001-add-ALPN-extension-support.patch added
Hi, I've attached a patch that adds ALPN support. I'll apply in a week if no one has objections!
Thanks!!

#8 - 07/15/2015 03:08 AM - normalperson (Eric Wong)
tenderlove@ruby-lang.org wrote:

```ruby
#ssl_alpn_select_cb(SSL *ssl, const unsigned char **out, unsigned char *outlen, const unsigned char *in, unsigned int inlen, void *arg)
+#{
+    int i = 0;
+    VALUE sslctx_obj, cb, protocols, selected;
+    sslctx_obj = (VALUE) arg;
+    cb = rb_iv_get(sslctx_obj, "@alpn_select_cb");
+    protocols = rb_ary_new();
+    /* The format is len_1|proto_1|...|len_n|proto_n\0 */
+    while (in[i]) {
+        VALUE protocol = rb_str_new((const char *) &in[i + 1], in[i]);
+        rb_ary_push(protocols, protocol);
+        i += in[i] + 1;
+    }
+    selected = rb_funcall(cb, rb_intern("call"), 1, protocols);
+   StringValue(selected);
+    *out = (unsigned char *)StringValuePtr(selected);
+    *outlen = RSTRING_LENINT(selected);
```

03/14/2022
I think we need to keep 'selected' markable by GC as long as anything may use 'out'. Otherwise 'out' can refer to a freed region.

Perhaps add the following here:

```c
rb_iv_set(sslctx_obj, "@_alpn_selected", selected);
```

Side note: StringValue is redundant if using StringValuePtr

Haven't looked at the rest closely, but that jumped out at me.

#9 - 07/15/2015 02:31 PM - tenderlovemaking (Aaron Patterson)
- File 0001-add-ALPN-extension-support.patch added

I think we need to keep 'selected' markable by GC as long as anything may use 'out'. Otherwise 'out' can refer to a freed region.

Perhaps add the following here:

```c
rb_iv_set(sslctx_obj, "@_alpn_selected", selected);
```

Side note: StringValue is redundant if using StringValuePtr

Thanks for spotting these! I've attached a new patch with these changes.

#10 - 07/17/2015 05:21 PM - tenderlovemaking (Aaron Patterson)
- File deleted (0001-add-ALPN-extension-support.patch)

#11 - 07/22/2015 06:32 PM - Anonymous
- Status changed from Assigned to Closed

Applied in changeset r51347.

- extopenssl/osssl_ssl.c: add ALPN support. [Feature #9390]
- extopenssl/extconf.rb: detect ALPN support in OpenSSL
- testopenssl/test_ssl.rb: test for ALPN

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-add-ALPN-extension-support.patch</td>
<td>7.78 KB</td>
<td>07/15/2015</td>
<td>tenderlovemaking (Aaron Patterson)</td>
</tr>
</tbody>
</table>