Ruby master - Bug #10533

HTTP reconnection with SNI does not send correct hostname

11/21/2014 03:41 AM - drbrain (Eric Hodel)

Status:	Closed		
Priority:	Normal		
Assignee:	drbrain (Eric Hodel)		
Target version:			
ruby -v:	ruby 2.1.5p273 (2014-11-13 revision 48405) [x86_64-darwin14.0]	**Backport:**	2.0.0: DONE, 2.1: DONE

Description

When reconnecting after connection timeout on an SNI connection the server name is not sent during reconnect which results in a failed reconnection:

```
$ cat test.rb
require 'net/http'
uri = URI 'https://david.shanske.com'

Net::HTTP.start uri.hostname, uri.port, use_ssl: true do |http|
  req = Net::HTTP::Get.new uri
  response = http.request req
  p response.code
  sleep 310
  req = Net::HTTP::Get.new uri
  response = http.request req
  p response.code
end
$ ruby -v test.rb
ruby 2.1.5p273 (2014-11-13 revision 48405) [x86_64-darwin14.0]
"200"
/usr/local/lib/ruby/2.1.0/openssl/ssl.rb:178:in `post_connection_check': hostname "david.shanske.c
om" does not match the server certificate (OpenSSL::SSL::SSLError)
        from /usr/local/lib/ruby/2.1.0/net/http.rb:922:in `connect'
        from /usr/local/lib/ruby/2.1.0/net/http.rb:1447:in `begin_transport'
        from /usr/local/lib/ruby/2.1.0/net/http.rb:1404:in `transport_request'
        from /usr/local/lib/ruby/2.1.0/net/http.rb:1378:in `request'
        from test.rb:10:in `block in <main>'
        from /usr/local/lib/ruby/2.1.0/net/http.rb:853:in `start'
        from /usr/local/lib/ruby/2.1.0/net/http.rb:583:in `start'
        from test.rb:4:in `<main>'
```

Related issues:

Related to Ruby master - Bug #10398: Server Name Indication support broken wh...	**Closed**

Associated revisions

Revision 711ece42 - 11/25/2014 07:09 AM - drbrain (Eric Hodel)

- lib/net/http.rb: Do not attempt SSL session resumption when the session is expired. [Bug #10533]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@48563 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 48563 - 11/25/2014 07:09 AM - drbrain (Eric Hodel)

- lib/net/http.rb: Do not attempt SSL session resumption when the session is expired. [Bug #10533]

Revision 48563 - 11/25/2014 07:09 AM - drbrain (Eric Hodel)

- lib/net/http.rb: Do not attempt SSL session resumption when the session is expired. [Bug #10533]

Revision 48563 - 11/25/2014 07:09 AM - drbrain (Eric Hodel)

- lib/net/http.rb: Do not attempt SSL session resumption when the session is expired. [Bug #10533]

Revision 48563 - 11/25/2014 07:09 AM - drbrain (Eric Hodel)

- lib/net/http.rb: Do not attempt SSL session resumption when the session is expired. [Bug #10533]

Revision 48563 - 11/25/2014 07:09 AM - drbrain (Eric Hodel)

- lib/net/http.rb: Do not attempt SSL session resumption when the session is expired. [Bug #10533]

Revision 48563 - 11/25/2014 07:09 AM - drbrain (Eric Hodel)

- lib/net/http.rb: Do not attempt SSL session resumption when the session is expired. [Bug #10533]

Revision dd7f1cdf - 11/28/2014 07:44 AM - usa (Usaku NAKAMURA)

merge revision(s) 48563: [Backport #10533]

```
    * lib/net/http.rb:  Do not attempt SSL session resumption when the
      session is expired.  [Bug #10533]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@48636 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 48636 - 11/28/2014 07:44 AM - usa (Usaku NAKAMURA)

merge revision(s) 48563: [Backport #10533]

```
* lib/net/http.rb:  Do not attempt SSL session resumption when the
  session is expired.  [Bug #10533]
```

Revision fd87a8ae - 02/17/2015 05:08 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r48563,r46261,r48581: [Backport #10533]

```
    * lib/net/http.rb:  Do not attempt SSL session resumption when the
      session is expired.  [Bug #10533]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@49631 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 49631 - 02/17/2015 05:08 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) r48563,r46261,r48581: [Backport #10533]

```
* lib/net/http.rb:  Do not attempt SSL session resumption when the
  session is expired.  [Bug #10533]
```

History

#1 - 11/21/2014 11:01 PM - drbrain (Eric Hodel)

- File net.http.bug10533.patch added

- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN to 2.0.0: REQUIRED, 2.1: REQUIRED

If session resumption is requested with an expired SSL session on an SNI server then the handshake goes wrong and the connection fails as above.

The attached patch only attempts session resumption if the session is still valid.

#2 - 11/21/2014 11:02 PM - drbrain (Eric Hodel)

- Status changed from Open to Assigned

- Assignee set to naruse (Yui NARUSE)

#3 - 11/22/2014 05:22 AM - drbrain (Eric Hodel)

Ultimately I think this may be an OpenSSL bug.

Looking at the ClientHello message for the second connection (which uses session resumption) no ServerNameIndication extension is present. Without this the server won't be able to respond with the correct certificate.

#4 - 11/25/2014 06:55 AM - drbrain (Eric Hodel)

- Assignee changed from naruse (Yui NARUSE) to drbrain (Eric Hodel)

Via #ruby-core IRC:

```
22:53 nurse: ok > 10533
```

So I will commit it.

#5 - 11/25/2014 07:09 AM - drbrain (Eric Hodel)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

Applied in changeset r48563.

- lib/net/http.rb: Do not attempt SSL session resumption when the session is expired. [Bug #10533]

#6 - 11/28/2014 07:44 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.0.0: REQUIRED, 2.1: REQUIRED to 2.0.0: DONE, 2.1: REQUIRED

Backported into ruby_2_0_0 at r48636.

#7 - 02/17/2015 05:09 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.0.0: DONE, 2.1: REQUIRED to 2.0.0: DONE, 2.1: DONE

r48563 and test for it (r46261,r48581) were backported into ruby_2_1 branch at r49631.

#8 - 06/12/2015 09:02 AM - mkarnebeek (Michiel Karnebeek)

The patch does not seem to solve the reported issue.

Reconnecting HTTP connections still do not send an SNI.

I'm running ruby 2.2.2p95 (2015-04-13 revision 50295) [x86_64-darwin14] and checked using Wireshark.

#9 - 06/17/2015 01:40 PM - mkarnebeek (Michiel Karnebeek)

Following up on my comment a few days ago:

I ran a test in python using https://github.com/nabla-c0d3/sslyze (with OpenSSL 1.0.2a, same version as in Ruby) and introduced a sleep longer than the ssl session TTL at https://github.com/nabla-c0d3/sslyze/blob/master/plugins/PluginSessionResumption.py#L248 to see if this did supply the SNI

According to Wireshark, this correctly put both the SNI and session ticket in the Client Hello packet.

I think this is evidence that the OpenSSL used is capable of doing this, and that either Net::Http or the c-bindings for ruby to OpenSSL are doing something wrong.

#10 - 06/18/2015 08:36 AM - mkarnebeek (Michiel Karnebeek)

- File net.http.bug10533-2.patch added

It looks like i've solved it: Moving s.hostname = @address before s.session = @ssl_session has solved it on my end.

See the attached patch

#11 - 06/18/2015 08:51 AM - mkarnebeek (Michiel Karnebeek)

Created https://github.com/ruby/ruby/pull/964

#12 - 06/18/2015 09:27 AM - mkarnebeek (Michiel Karnebeek)

Root cause seems to be in ossl_ssl.c:

Net::Http calls s.session= (C-method ossl_ssl_set_session), which calls C-method ossl_ssl_setup, which only sets up the ssl client (ssl) once due to "if(!ssl){". The problem is that the hostname setting (the call to SSL_set_tlsext_host_name) is done within that "if(!ssl){" block.

When later Net::Http calls s.connect (C-method ossl_ssl_connect), ossl_ssl_setup is called a second time, but it does not set up the hostname.

#13 - 06/24/2015 08:41 AM - a.holstvoogd (Arthur Holstvoogd)

Related i.e same issue: #10398

#14 - 07/09/2015 06:56 AM - naruse (Yui NARUSE)

- Related to Bug #10398: Server Name Indication support broken when reusing a (dead) session added

Files

net.http.bug10533.patch	685 Bytes	11/21/2014	drbrain (Eric Hodel)
net.http.bug10533-2.patch	884 Bytes	06/18/2015	mkarnebeek (Michiel Karnebeek)