

Ruby - Bug #4923

[ext/openssl] test_ssl.rb: test_client_auth fails

06/23/2011 11:48 PM - MartinBosslet (Martin Bosslet)

Status:	Closed	Backport:
Priority:	Normal	
Assignee:	MartinBosslet (Martin Bosslet)	
Target version:		
ruby -v:	ruby 1.9.3dev (2011-06-13 trunk 32213) [i686-linux]	
Description		
Hi,		
I was finally able to reproduce this with Fedora 15 32 bit, OpenSSL 1.0.0d.		
The error occurs only when running make test-all TESTS="openssl", if I run test_ssl.rb independently the test succeeds.		
Here is the output I get:		
1. Error: test_client_auth(OpenSSL::TestSSL): OpenSSL::SSL::SSLReadError: SSL_read:: sslv3 alert bad record mac /home/martin/Projekte/Ruby/build/.ext/common/openssl/buffering.rb:53:in sysread' /home/martin/Projekte/Ruby/build/.ext/common/openssl/buffering.rb:53:in fill_rbuff' /home/martin/Projekte/Ruby/build/.ext/common/openssl/buffering.rb:200:in gets' /home/martin/Projekte/Ruby/ruby/test/openssl/test_ssl.rb:118:in block in test_client_auth' /home/martin/Projekte/Ruby/ruby/test/openssl/utls.rb:280:in call' /home/martin/Projekte/Ruby/ruby/test/openssl/utls.rb:280:in start_server' /home/martin/Projekte/Ruby/ruby/test/openssl/test_ssl.rb:103:in `test_client_auth'		
Related to #4919 .		
Regards, Martin		
Related issues:		
Related to Ruby - Bug #4919: OpenSSL::SSL::Sesssion#time= Bignum [] Argum...		Closed 06/22/2011

History

#1 - 06/24/2011 04:42 AM - MartinBosslet (Martin Bosslet)

- Priority changed from Normal to 3

Strange. I tried with 0.9.8r, couldn't reproduce it. Then I tried with 1.0.0d, again the tests succeeded. It is only the customized version of 1.0.0d that ships with Fedora 15 that causes the error. I know that they disabled ECC support in their version of OpenSSL 1.0.0d, so they possibly changed other things, too, that could cause the failure.

I'll investigate this further.

#2 - 06/24/2011 10:04 PM - MartinBosslet (Martin Bosslet)

- Assignee set to nahi (Hiroshi Nakamura)

I played around a bit and it seems like this could be some kind of race condition. At first I thought that the custom Fedora OpenSSL would probably reject some algorithm and so I wanted to see what cipher is negotiated in the tests and added this:

Index: test/openssl/utls.rb

--- test/openssl/utls.rb (revision 32218)
+++ test/openssl/utls.rb (working copy)

@@ -226,6 +226,7 @@

```
ssl = nil
begin
ssl = ssls.accept
```

```
• [REDACTED]
  rescue OpenSSL::SSL::SSLError
    retry
  end
```

This actually made the test failure disappear.

It also disappears if I leave some of the openssl tests out, e.g. if I leave out the first test test_asn.rb or test_cipher.rb - this will also cause test_ssl.rb to succeed. What bugs me is that these tests aren't related to test_ssl.rb except maybe for the fact that they all "require openssl" and utils.rb. Could it be that something persists in the buffer used for the SSL tests that is introduced by any of the other tests?

It's really weird... Hiroshi, do you have an idea what the cause might be?

I would tend to ignore this since it only appears with a customized OpenSSL version in a very specific scenario if it weren't for the fact that I'm afraid if really a race condition is the problem then this could also come up again in other situations...

Thanks in advance,
Martin

#3 - 06/26/2011 07:21 PM - nahi (Hiroshi Nakamura)

- Target version set to 1.9.3

#4 - 06/28/2011 03:40 AM - MartinBosslet (Martin Bosslet)

Not sure if it is related:

I tested again using Ubuntu 10.04 with OpenSSL 0.9.8k and make test-all TESTS="openssl/test_pair.rb" (at r32258) and I get this (reproducible all the time):

Running tests:

.....E.

Finished tests in 1.201981s, 16.6392 tests/s, 84.0280 assertions/s.

1. Error:

```
test_write_nonblock(OpenSSL::TestPair):
OpenSSL::SSL::SSLError: SSL_read:: bad write retry
/home/martin/Projekte/Ruby/ruby-svn/build/.ext/common/openssl/buffering.rb:53:in sysread'
/home/martin/Projekte/Ruby/ruby-svn/build/.ext/common/openssl/buffering.rb:53:in fill_rbuff'
/home/martin/Projekte/Ruby/ruby-svn/build/.ext/common/openssl/buffering.rb:94:in read'
/home/martin/Projekte/Ruby/ruby-svn/ruby/test/openssl/test_pair.rb:176:in block in test_write_nonblock'
/home/martin/Projekte/Ruby/ruby-svn/ruby/test/openssl/test_pair.rb:44:in ssl_pair'
/home/martin/Projekte/Ruby/ruby-svn/ruby/test/openssl/test_pair.rb:164:in test_write_nonblock'
```

20 tests, 101 assertions, 0 failures, 1 errors, 0 skips

However, when running the test with OpenSSL 1.0.0d on the same machine, it succeeds.

#5 - 06/28/2011 04:40 AM - MartinBosslet (Martin Bosslet)

Martin Bosslet wrote:

1. Error:

```
test_write_nonblock(OpenSSL::TestPair):
OpenSSL::SSL::SSLError: SSL_read:: bad write retry
/home/martin/Projekte/Ruby/ruby-svn/build/.ext/common/openssl/buffering.rb:53:in sysread'
/home/martin/Projekte/Ruby/ruby-svn/build/.ext/common/openssl/buffering.rb:53:in fill_rbuff'
/home/martin/Projekte/Ruby/ruby-svn/build/.ext/common/openssl/buffering.rb:94:in read'
/home/martin/Projekte/Ruby/ruby-svn/ruby/test/openssl/test_pair.rb:176:in block in test_write_nonblock'
/home/martin/Projekte/Ruby/ruby-svn/ruby/test/openssl/test_pair.rb:44:in ssl_pair'
```

/home/martin/Projekte/Ruby/ruby-svn/ruby/test/openssl/test_pair.rb:164:in test_write_nonblock'

20 tests, 101 assertions, 0 failures, 1 errors, 0 skips

I tested further and the test fails deterministically at the same spot each time. If I rewrite test_write_nonblock as follows:

```
def test_write_nonblock
  ssl_pair {|s1, s2|
    n = 0
    begin
      n += s1.write_nonblock("a" * 100000)
      n += s1.write_nonblock("b" * 100000)
      n += s1.write_nonblock("c" * 100000)
      100000.times do |i|
        n += 1
        begin
          s1.write_nonblock("d")
        rescue OpenSSL::SSL::SSLError => e
          p e
          puts "Iteration: #{i}"
          raise e
        end
      end
    end
    puts "Da5"
    n += s1.write_nonblock("e" * 100000)
    puts "Da6"
    n += s1.write_nonblock("f" * 100000)
    puts "Da7"
  rescue IO::WaitWritable
  end
  s1.close
  assert_equal(n, s2.read.length)
}
```

end

it will always yield the same result (only with Ubuntu's 0.9.8k though) when running make test-all TESTS="openssl/test_pair.rb":

```
.....#<OpenSSL::SSL::SSLError: write would block>
Iteration: 441
E.
```

Finished tests in 1.213241s, 16.4848 tests/s, 83.2481 assertions/s.

1. Error:

```
test_write_nonblock(OpenSSL::TestPair):
OpenSSL::SSL::SSLError: SSL_read:: bad write retry
/home/martin/Projekte/Ruby/ruby-svn/build/.ext/common/openssl/buffering.rb:53:in sysread'
/home/martin/Projekte/Ruby/ruby-svn/build/.ext/common/openssl/buffering.rb:53:in fill_rbuff'
/home/martin/Projekte/Ruby/ruby-svn/build/.ext/common/openssl/buffering.rb:94:in read'
/home/martin/Projekte/Ruby/ruby-svn/ruby/test/openssl/test_pair.rb:188:in block in test_write_nonblock'
/home/martin/Projekte/Ruby/ruby-svn/ruby/test/openssl/test_pair.rb:44:in ssl_pair'
/home/martin/Projekte/Ruby/ruby-svn/ruby/test/openssl/test_pair.rb:164:in test_write_nonblock'
```

20 tests, 101 assertions, 0 failures, 1 errors, 0 skips

It always flunks at iteration 441 with an "OpenSSL::SSL::SSLError: write would block".

#6 - 06/29/2011 04:30 PM - nahi (Hiroshi Nakamura)

- Priority changed from 3 to Normal

Great. Thanks. I changed the priority since Martin found the way to replicate. What makes the story more interesting is that the test 'test_write_nonblock' does not give me a SSLError but an assertion failure at the last assert.

I'll investigate it.

#7 - 06/29/2011 05:52 PM - nahi (Hiroshi Nakamura)

The failure I was getting is from the wrong place of 'n += 1'. So it just means 1.0.0d is safe. And I can replicate the error with 0.9.8o on Ubuntu 11.04

Martin, can you add a SSLSocket#close call for s1 and s2 in 'test_connect_accept_nonblock' ensure block, then try the test again? This looks hide the error for me (run all tests normally.)

#8 - 06/30/2011 11:21 AM - MartinBosslet (Martin Bosslet)

Oops, the n += 1 was misplaced indeed :)

I tried on Fedora 15 with the official 0.9.8k and was able to reproduce the error in 'test_write_non_block'. Closing sockets s1 and s2 in the ensure block in 'test_connect_accept_nonblock' unfortunately didn't help, still the same error (running the tests normally).

Next, I tested with 0.9.8o (official download) and *wasn't* able to reproduce it (again Fedora 15 32 bit) - in contrast to your experience.

0.9.8k: Fails
0.9.8l: Fails
0.9.8m: Succeeds
0.9.8n: Succeeds
0.9.8o: Succeeds
0.9.8r: Succeeds
1.0.0d: Succeeds

So it seems that on my side I'm able to reproduce it deterministically with 0.9.8k and 0.9.8l, but the failure vanishes in versions >= 0.9.8m.

I scanned through OpenSSL's change log looking for changes made in 0.9.8m and found this:

Handle non-blocking I/O properly in SSL_shutdown() call.
[Darryl Miles darryl-mailinglists@netbauds.net]

The behavior on my machine would underline the assumption that this is probably the cause. What do you think? Should I try to find out exactly what Darryl Miles changed to see whether we could handle this in ext/openssl, too?

#9 - 07/11/2011 03:08 PM - kosaki (Motohiro KOSAKI)

- Status changed from Open to Assigned

#10 - 07/12/2011 06:18 PM - nahi (Hiroshi Nakamura)

- Priority changed from Normal to 3

I'm on 64bit Ubuntu 11.04 box, and I can replicate the error with 0.9.8o...

Though we still don't know the culprit of this failure, I mark this Low-priority since it's not a report from user.

Martin, you can change Assignee and take this as you like :)

#11 - 07/13/2011 07:21 PM - MartinBosslet (Martin Bosslet)

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

Martin, you can change Assignee and take this as you like :)

Thanks, Hiroshi!

If I get [#4961](#) done in time I will also try to have this fixed for the 1.9.3 release.

#12 - 07/25/2011 12:43 PM - nahi (Hiroshi Nakamura)

While investigating [#5039](#), I found that SSL_shutdown() could add something to global error stack in OpenSSL < 0.9.8m, possibly related the OpenSSL 0.9.8m fix Martin posted above. Based on my investigation, that's the reason why 'bad write retry' (error for SSL_write) is raised from SSL_read. I'll handle 'bad write retry' for SSL_read issue at [#5039](#).

It explains the error 'bad write retry' we're getting well but it doesn't for the error 'SSL_read:: sslv3 alert bad record mac' so I keep this ticket for the issue 'SSL_read:: sslv3 alert bad record mac'.

Martin, do you have any thought about the original error? Are you still getting the error? (not 'bad write retry')

#13 - 07/27/2011 07:39 AM - MartinBosslet (Martin Bosslet)

Hiroshi Nakamura wrote:

While investigating [#5039](#), I found that SSL_shutdown() could add something to global error stack in OpenSSL < 0.9.8m, possibly related the OpenSSL 0.9.8m fix Martin posted above. Based on my investigation, that's the reason why 'bad write retry' (error for SSL_write) is raised from SSL_read. I'll handle 'bad write retry' for SSL_read issue at [#5039](#).

Runs smooth now with all OpenSSL versions that previously produced the 'bad write retry'. Great work!

It explains the error 'bad write retry' we're getting well but it doesn't for the error 'SSL_read:: sslv3 alert bad record mac' so I keep this ticket for the issue 'SSL_read:: sslv3 alert bad record mac'.

Martin, do you have any thought about the original error? Are you still getting the error? (not 'bad write retry')

I don't know what I did to produce that thing. That night I was able to reproduce it just fine, but I never got it again since then. I just ran make test-all for openssl with the custom Fedora version 50 times, not a single error.

What should we do, close it? We could still reopen the issue if I somehow manage to reproduce it...

Since I didn't (and don't) know where to look for it, debugging hasn't led me any further for now - I'm still clueless concerning the origin of the 'bad record mac'.

#14 - 07/28/2011 04:41 PM - nahi (Hiroshi Nakamura)

- Status changed from Assigned to Feedback

- Assignee deleted (MartinBosslet (Martin Bosslet))

- Target version deleted (1.9.3)

Martin Bosslet wrote:

I don't know what I did to produce that thing. That night I was able to reproduce it just fine, but I never got it again since then. I just ran make test-all for openssl with the custom Fedora version 50 times, not a single error.

What should we do, close it? We could still reopen the issue if I somehow manage to reproduce it...

Thanks for confirmation. Let's mark this ticket state as 'Feedback'.

#15 - 10/31/2012 12:57 AM - mame (Yusuke Endoh)

Martin and NaHi,

Is there any concrete plan to address this issue?

If not, I'd like to close this ticket now.

You can reopen it whenever you find any clue to make a progres.

--

Yusuke Endoh mame@tsg.ne.jp

#16 - 11/05/2012 10:57 PM - mame (Yusuke Endoh)

- Assignee set to MartinBosslet (Martin Bosslet)

Emboss and NaHi, ping?

--

Yusuke Endoh mame@tsg.ne.jp

#17 - 11/21/2012 11:02 AM - MartinBosslet (Martin Bosslet)

mame (Yusuke Endoh) wrote:

Emboss and NaHi, ping?

--

If nahi agrees, I would say "close" since no feedback arrived in the meantime?

#18 - 01/26/2013 06:51 AM - drbrain (Eric Hodel)

- Status changed from Feedback to Closed

I am closing this due to lack of feedback and the note of a possible fix above.